(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007623 A2

(51) International Patent Classification[7]: H04Q 1/00, G05B 19/00

(21) International Application Number: PCT/US02/21903

(22) International Filing Date: 10 July 2002 (10.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/304,216 10 July 2001 (10.07.2001) US

(71) Applicant: **AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPAGNY, INC** [US/US]; American Express Tower, World Financial Center, New York, NY 10285-4900 (US).

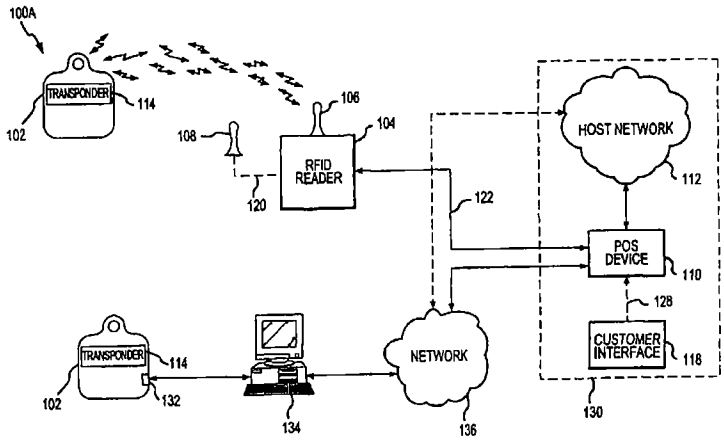
(72) Inventors: **BERARDI, Michael, J.**; 7770 NW 50th Street, #306, Lauderhill, FL 33313 (US). **BLIMAN, Michal**; 4 Dogwood Circle, Matawan, NJ 07747 (US). **BONALLE, David, S.**; 77 Rose Hill Avenue, New Rochelle, NY 10804 (US). **ELWOOD, Jennifer, Anne**; 115 East 34th Street, Apt. #8-G, New York City, NY 10016 (US). **HOOD, Matthew, C.**; 1112 LaFayette Road, Wayne, PA 19087 (US). **ISENBERG, Susan, E.**; 201 West 74 th, 12 th, New York City, NY 10012 (US). **MAYERS, Alexandra**; 49 Grove Street, #5-B, New York City, NY 10014 (US). **SAUNDERS, Peter, D.**; 3710 East Palisade Drive, Salt Lake City, UT 84109 (US). **SCHEDING, Kathryn, D.**; 12301 Clover Avenue, Los Angeles, CA 90066 (US). **SHAH, Sejal, Ajit**; 230 East 30th Street, #11-J, New York City, NY 10016 (US). **WILLIAMSON, John, R.**; 302 Pavonia Avenue, Jersey City, NJ 07302 (US).

(74) Agent: **SOBELMAN, Howard, I.**; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS



(57) Abstract: A transporter-reader payment system includes a fob including a transponder, and a RFID reader for interrogating the transponder. The system may further include a personalization system for populating onto the fob and RFID reader identifying information and security and authentification keys which may be used during mutual authentication of the fob and the reader and for completing a transaction. In exemplary operation, the fob and RFID reader may be personalized, the fob may be presented to the RFID reader for interrogation, the fob and reader may engage in mutual authhentication, and fob identifying information may be provided to the reader for transaction completion. In another exemplary embodiment, operation of the transponder-reader payment system may be controlled by an activation circuit. Further, the fob may be responsive to multiple interrogation signals.

WO 03/007623 A2

SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS

Field of Invention

This invention generally relates to a system and method for completing a transaction, and more particularly, to completing a financial transaction using Radio Frequency Identification (RFID) in contact and contactless transactions.

Background of the Invention

Like barcode and voice data entry, RFID is a contactless information acquisition technology. RFID systems are wireless, and are usually extremely effective in hostile environments where conventional acquisition methods fail. RFID has established itself in a wide range of markets, such as, for example, the high-speed reading of railway containers, tracking moving objects such as livestock or automobiles, and retail inventory applications. As such, RFID technology has become a primary focus in automated data collection, identification and analysis systems worldwide.

Of late, companies are increasingly embodying RFID data acquisition technology in a fob or tag for use in completing financial transactions. A typical fob includes a transponder and is ordinarily a self-contained device which may be contained on any portable form factor. In some instances, a battery may be included with the fob to power the transponder. In which case the internal circuitry of the fob (including the transponder) may draw its operating power from the battery power source. Alternatively, the fob may exist independent of an internal power source. In this instance the internal circuitry of the fob (including the transponder) may gain its operating power directly from an RF interrogation signal. U.S. Patent No. 5,053,774 issued to Schuermann describes a typical transponder RF interrogation system which may be found in the prior art. The Schuermann patent describes in general the powering technology surrounding conventional transponder structures. U.S. Patent No. 4,739,328 discusses a method by which a conventional transponder may respond to a RF interrogation signal. Other typical modulation techniques which may be used include, for example, ISO/IEC 14443 and the like.

In the conventional fob powering technologies used, the fob is typically activated upon presenting the fob in an interrogation signal. In this regard, the fob may be activated irrespective of whether the user desires such activation. Inadvertent presentation of the fob may result in initiation and completion of an unwanted transaction. Thus, a fob system is needed which allows the fob user to control activation of the fob to limit transactions being undesirably completed.

One of the more visible uses of the RFID technology is found in the introduction of Exxon/Mobil's Speedpass® and Shell's EasyPay® products. These products use transponders placed in a fob or tag which enables automatic identification of the user when the fob is presented at a Point of Sale (POS) device. Fob identification data is typically passed to a third party server database, where the identification data is referenced to a customer (*e.g.*, user) credit or debit account. In an exemplary processing method, the server seeks authorization for the transaction by passing the transaction and account data to an authorizing entity. Once authorization is received by the server, clearance is sent to the point of sale device for completion of the transaction. In this way, the conventional transaction processing method involves an indirect path which causes undue overhead due to the use of the third-party server.

A need exists for a transaction authorization system which allows Fob transactions to be authorized while eliminating the cost associated with using third-party servers.

In addition, conventional fobs are limited in that they must be used in proximity to the Point of Sale device. That is, for fob activation, conventional fobs must be positioned within the area of transmission cast by the RF interrogation signal. More particularly, conventional fobs are not affective for use in situations where the user wishes to conduct a transaction at a point of interaction such as a computer interface.

Therefore, a need exists for a fob embodying RFID acquisition technology, which is capable of use at a point of sale device and which is additionally capable of facilitating transactions via a computer interface connected to a network (*e.g.*, the Internet).

Existing transponder-reader payment systems are also limited in that the conventional fob used in the systems is only responsive to one interrogation signal.

Thus, where multiple interrogation signals are used, the fob is only responsive to the interrogation signal to which it is configured. If the RFID reader of the system provides only an interrogation signal to which the fob is incompatible, the fob will not be properly activated.

Therefore, a need exists for a fob which is responsive to more than one interrogation signal.

Summary of the Invention

Described herein is a system and method for using RFID technology to initiate and complete financial transactions. The transponder-reader payment system described herein may include a RFID reader operable to provide a RF interrogation signal for powering a transponder system, receiving a transponder system RF signal, and providing transponder system account data relative to the transponder system RF signal. The transponder-reader payment system may include a RFID protocol/sequence controller in electrical communication with one or more interrogators for providing an interrogation signal to a transponder, a RFID authentication circuit for authenticating the signal received from the transponder, a serial or parallel interface for interfacing with a point of interaction device, and an USB or serial interface for use in personalizing the RFID reader and/or the transponder. The transponder-reader payment system may further include a fob including one or more transponders (*e.g.*, modules) responsive to the interrogation signal and for providing an authentication signal for verifying that the transponder and/or the RFID reader are authorized to operate within the transponder-reader payment system. In this way, the transponder may be responsive to multiple interrogation signals provided at different frequencies. Further, the transponder may include a USB or serial interface for use with a computer network or with the RFID reader.

The RFID system and method according to the present invention may include a RFID-ready terminal and a transponder which may be embodied in a fob, tag, card or any other form factor (*e.g.*, wristwatch, keychain, cell phone, etc.), which may be capable of being presented for interrogation. In that regard, although the transponder is described herein as embodied in a fob, the invention is not so limited.

The system may further include a RFID reader configured to send a standing RFID recognition signal which may be transmitted from the RFID reader via radio frequency (or electromagnetic) propagation. The fob may be placed within proximity to the RFID reader such that the RFID signal may interrogate the fob and initialize fob identification procedures.

In one exemplary embodiment, as a part of the identification process, the fob and the RFID reader may engage in mutual authentication. The RFID reader may identify the fob as including an authorized system transponder for receiving encrypted information and storing the information on the fob memory. Similarly, the fob, upon interrogation by the RFID reader, may identify the RFID reader as authorized to receive the encrypted and stored information. Where the RFID reader and the fob successfully mutually authenticate, the fob may transmit to the RFID reader certain information identifying the transaction account or accounts to which the fob is associated. The RFID reader may receive the information and forward the information to facilitate the completion of a transaction. In one exemplary embodiment, the RFID reader may forward the information to a point of interaction device (*e.g.*, POS or computer interface) for transaction completion. The mutual authorization process disclosed herein aids in ensuring fob transponder-reader payment system security.

In another exemplary embodiment, the fob according to the present invention, includes means for completing transactions via a computer interface. The fob may be connected to the computer using a USB or serial interface fob account information may be transferred to the computer for use in completing a transaction via a network (*e.g.*, the Internet).

These features and other advantages of the system and method, as well as the structure and operation of various exemplary embodiments of the system and method, are described below.

Brief Description of the Drawings

The accompanying drawings, wherein like numerals depict like elements, illustrate exemplary embodiments of the present invention, and together with the description, serve to explain the principles of the invention. In the drawings:

FIG. 1A illustrates an exemplary RFID-based system in accordance with the present invention, wherein exemplary components used for fob transaction completion are depicted;

FIG. 1B illustrates an exemplary personalization system in accordance with the present invention;

FIG. 2 is a schematic illustration of an exemplary fob in accordance with the present invention;

FIG. 3 is a schematic illustration of an exemplary RFID reader in accordance with the present invention;

FIG. 4 is an exemplary flow diagram of an exemplary authentication process in accordance with the present invention;

FIG. 5 is an exemplary flow diagram of an exemplary decision process for a protocol/sequence controller in accordance with the present invention;

FIGS. 6A-B are an exemplary flow diagram of a fob personalization process in accordance with the present invention;

FIGS. 7A-B are an exemplary flow diagram of a RFID reader personalization process in accordance with the present invention;

FIG. 8 is a flow diagram of an exemplary payment/transaction process in accordance with the present invention; and

FIG. 9 is another schematic illustration of an exemplary fob in accordance with the present invention.

Detailed Description

The present invention may be described herein in terms of functional block components, screen shots, optional selections and various processing steps. Such functional blocks may be realized by any number of hardware and/or software components configured to perform to specified functions. For example, the present invention may employ various integrated circuit components, *e.g.*, memory elements, processing elements, logic elements, look-up tables, and the like, which may carry out a variety of functions under the control of one or more mircroprocessors or other control devices. Similarly, the software elements of the present invention may be implemented with any programming or scripting language such as C, C++, Java, COBOL, assembler, PERL, extensible markup language

(XML), JavaCard and MULTOS with the various algorithms being implemented with any combination of data structures, objects, processes, routines or other programming elements. Further, it should be noted that the present invention may employ any number of conventional techniques for data transmission, signaling, data processing, network control, and the like. For a basic introduction on cryptography, review a text written by Bruce Schneier entitled "Applied Cryptography: Protocols, Algorithms, and Source Code in C," published by John Wiley & Sons (second edition, 1996), herein incorporated by reference.

In addition, many applications of the present invention could be formulated. The exemplary network disclosed herein may include any system for exchanging data or transacting business, such as the internet, an intranet, an extranet, WAN, LAN, satellite communications, and/or the like. It is noted that the network may be implemented as other types of networks, such as an interactive television network (ITN).

Where required, the system user may interact with the system via any input device such as, a keypad, keyboard, mouse, kiosk, personal digital assistant, handheld computer (*e.g.*, Palm Pilot®, Blueberry®), cellular phone and/or the like. Similarly, the invention could be used in conjunction with any type of personal computer, network computer, work station, minicomputer, mainframe, or the like running any operating system such as any version of Windows, Windows NT, Windows 2000, Windows 98, Windows 95, MacOS, OS/2, BeOS, Linux, UNIX, Solaris or the like. Moreover, although the invention may frequently be described as being implemented with TCP/IP communications protocol, it should be understood that the invention could also be implemented using SNA, IPX, Appletalk, IPte, NetBIOS, OSI or any number of communications protocols. Moreover, the system contemplates, the use, sale, or distribution of any goods, services or information over any network having similar functionality described herein.

FIG. 1A illustrates an exemplary RFID transaction system 100A in accordance with the present invention, wherein exemplary components for use in completing a fob transaction are depicted. In general, the operation of system 100A may begin when fob 102 is presented for payment, and is interrogated by RFID reader 104 or, alternatively, interface 134. Fob 102 and RFID reader 104 may then engage in mutual authentication after which the transponder 102 may provide the

transponder identification and/or account identifier to the RFID reader 104 which may further provide the information to the merchant system 130 POS device 110.

System 100A may include a fob 102 having a transponder 114 and a RFID reader 104 in RF communication with fob 102. Although the present invention is described with respect to a fob 102, the invention is not to be so limited. Indeed, system 100 may include any device having a transponder which is configured to communicate with a RFID reader 104 via RF communication. Typical devices may include, for example, a key ring, tag, card, cell phone, wristwatch or any such form capable of being presented for interrogation.

The RFID reader 104 may be configured to communicate using a RFID internal antenna 106. Alternatively, RFID reader 104 may include an external antenna 108 for communications with fob 102, where the external antenna may be made remote to the RFID reader 104 using a suitable cable and/or data link 120. RFID reader 104 may be further in communication with a merchant system 130 via a data link 122. The system 100A may include a transaction completion system including a point of interaction device such as, for example, a merchant point of sale (POS) device 110 or a computer interface (*e.g.*, user interface) 134. In one exemplary embodiment the transaction completion system may include a merchant system 130 including the POS device 110 in communication with a RFID reader 104 (via data link 122). As described more fully below, the transaction completion system may include the user interface 134 connected to a network 136 and to the transponder via a USB connector 132.

Although the point of interaction device is described herein with respect to a merchant point of sale (POS) device, the invention is not to be so limited. Indeed, a merchant POS device is used herein by way of example, and the point of interaction device may be any device capable of receiving fob account data. In this regard, the POS may be any point of interaction device enabling the user to complete a transaction using a fob 102. POS device 110 may be in further communication with a customer interface 118 (via data link 128) for entering at least a customer identity verification information. In addition, POS device 110 may be in communication with a merchant host network 112 (via data link 124) for processing any transaction request. In this arrangement, information provided by RFID reader 104 is provided to the POS device 110 of merchant system 130 via data link 122. The POS device

110 may receive the information (and alternatively may receive any identity verifying information from customer interface 118 via data link 128) and provide the information to host system 112 for processing.

A variety of conventional communications media and protocols may be used for data links 120, 122, 124, and 128. For example, data links 120, 122, 124, and 128 may be an Internet Service Provider (ISP) configured to facilitate communications over a local loop as is typically used in connection with standard modem communication, cable modem, dish networks, ISDN, Digital Subscriber Lines (DSL), or any wireless communication media. In addition, the merchant system 130 including the POS device 110 and host network 112 may reside on a local area network which interfaces to a remote network (not shown) for remote authorization of an intended transaction. The merchant system 130 may communicate with the remote network via a leased line, such as a T1, D3 line, or the like. Such communications lines are described in a variety of texts, such as, "Understanding Data Communications," by Gilbert Held, which is incorporated herein by reference.

An account number, as used herein, may include any identifier for an account (*e.g.*, credit, charge debit, checking, savings, reward, loyalty, or the like) which may be maintained by a transaction account provider (*e.g.*, payment authorization center) and which may be used to complete a financial transaction. A typical account number (*e.g.*, account data) may be correlated to a credit or debit account, loyalty account, or rewards account maintained and serviced by such entities as American Express, Visa and/or MasterCard or the like. For ease in understanding, the present invention may be described with respect to a credit account. However, it should be noted that the invention is not so limited and other accounts permitting an exchange of goods and services for an account data value is contemplated to be within the scope of the present invention.

In addition, the account number (*e.g.*, account data) may be associated with any device, code, or other identifier/indicia suitably configured to allow the consumer to interact or communicate with the system, such as, for example, authorization/access code, personal identification number (PIN), Internet code, digital certificate, biometric data, and/or other identification indicia. The account number may be optionally located on a rewards card, charge card, credit card, debit

card, prepaid card, telephone card, smart card, magnetic stripe card, bar code card, and/or the like. The account number may be distributed and stored in any form of plastic, electronic, magnetic, and/or optical device capable of transmitting or downloading data to a second device. A customer account number may be, for example, a sixteen-digit credit card number, although each credit provider has its own numbering system, such as the fifteen-digit numbering system used by American Express. Each company's credit card numbers comply with that company's standardized format such that the company using a sixteen-digit format will generally use four spaced sets of numbers, as represented by the number "0000 0000 0000 0000". In a typical example, the first five to seven digits are reserved for processing purposes and identify the issuing bank, card type and etc. In this example, the last sixteenth digit is used as a sum check for the sixteen-digit number. The intermediary eight-to-ten digits are used to uniquely identify the customer. The account number stored as Track 1 and Track 2 data as defined in ISO/IEC 7813, and further may be made unique to fob 102. In one exemplary embodiment, the account number may include a unique fob serial number and user identification number, as well as specific application applets. The account number may be stored in fob 102 inside a database 214, as described more fully below. Database 214 may be configured to store multiple account numbers issued to the fob 102 user by the same or different account providing institutions. Where the account data corresponds to a loyalty or rewards account, the database 214 may be configured to store the attendant loyalty or rewards points data.

FIG. 2 illustrates a block diagram of the many functional blocks of an exemplary fob 102 in accordance with the present invention. Fob 102 may be a RFID fob 102 which may be presented by the user to facilitate an exchange of funds or points, etc., for receipt of goods or services. As described herein, by way of example, the fob 102 may be a RFID fob which may be presented for facilitating payment for goods and/or services.

Fob 102 may include an antenna 202 for receiving an interrogation signal from RFID reader 104 via antenna 106 (or alternatively, via external antenna 108). Fob antenna 202 may be in communication with a transponder 114. In one exemplary embodiment, transponder 114 may be a 13.56 MHz transponder compliant with the ISO/IEC 14443 standard, and antenna 202 may be of the 13 MHz

variety. The transponder 114 may be in communication with a transponder compatible modulator/demodulator 206 configured to receive the signal from transponder 114 and configured to modulate the signal into a format readable by any later connected circuitry. Further, modulator/demodulator 206 may be configured to format (*e.g.*, demodulate) a signal received from the later connected circuitry in a format compatible with transponder 114 for transmitting to RFID reader 104 via antenna 202. For example, where transponder 114 is of the 13.56 MHz variety, modulator/demodulator 206 may be ISO/IEC 14443-2 compliant.

Modulator/demodulator 206 may be coupled to a protocol/sequence controller 208 for facilitating control of the authentication of the signal provided by RFID reader 104, and for facilitating control of the sending of the fob 102 account number. In this regard, protocol/sequence controller 208 may be any suitable digital or logic driven circuitry capable of facilitating determination of the sequence of operation for the fob 102 inner-circuitry. For example, protocol/sequence controller 208 may be configured to determine whether the signal provided by the RFID reader 104 is authenticated, and thereby providing to the RFID reader 104 the account number stored on fob 102.

Protocol/sequence controller 208 may be further in communication with authentication circuitry 210 for facilitating authentication of the signal provided by RFID reader 104. Authentication circuitry may be further in communication with a non-volatile secure memory database 212. Secure memory database 212 may be any suitable elementary file system such as that defined by ISO/IEC 7816-4 or any other elementary file system allowing a lookup of data to be interpreted by the application on the chip. Database 212 may be any type of database, such as relational, hierarchical, object-oriented, and/or the like. Common database products that may be used to implement the databases include DB2 by IBM (White Plains, NY), any of the database products available from Oracle Corporation (Redwood Shores, CA), Microsoft Access or MSSQL by Microsoft Corporation (Redmond, Washington), or any other database product. Database may be organized in any suitable manner, including as data tables or lookup tables. Association of certain data may be accomplished through any data association technique known and practiced in the art. For example, the association may be accomplished either manually or automatically. Automatic association techniques may include, for

example, a database search, a database merge, GREP, AGREP, SQL, and/or the like. The association step may be accomplished by a database merge function, for example, using a "key field" in each of the manufacturer and retailer data tables. A "key field" partitions the database according to the high-level class of objects defined by the key field. For example, a certain class may be designated as a key field in both the first data table and the second data table, and the two data tables may then be merged on the basis of the class data in the key field. In this embodiment, the data corresponding to the key field in each of the merged data tables is preferably the same. However, data tables having similar, though not identical, data in the key fields may also be merged by using AGREP, for example.

The data may be used by protocol/sequence controller 208 for data analysis and used for management and control purposes, as well as security purposes. Authentication circuitry may authenticate the signal provided by RFID reader 104 by association of the RFID signal to authentication keys stored on database 212. Encryption circuitry may use keys stored on database 212 to perform encryption and/or decryption of signals sent to or from the RFID reader 104.

In addition, protocol/sequence controller 208 may be in communication with a database 214 for storing at least a fob 102 account data, and a unique fob 102 identification code. Protocol/sequence controller 208 may be configured to retrieve the account number from database 214 as desired. Database 214 may be of the same configuration as database 212 described above. The fob account data and/or unique fob identification code stored on database 214 may be encrypted prior to storage. Thus, where protocol/sequence controller 208 retrieves the account data, and or unique fob identification code from database 214, the account number may be encrypted when being provided to RFID reader 104. Further, the data stored on database 214 may include, for example, an unencrypted unique fob 102 identification code, a user identification, Track 1 and 2 data, as well as specific application applets.

Fob 102 may be configured to respond to multiple interrogation frequency transmissions provided by RFID reader 104. That is, as described more fully below, RFID reader 104 may provide more than one RF interrogation signal. In this case, fob 102 may be configured to respond to the multiple frequencies by including in fob 102 one or more additional RF signal receiving/transmitting units 226. RF signal

receiving/transmitting unit 226 may include an antenna 218 and transponder 220 where the antenna 218 and transponder 220 are compatible with at least one of the additional RF signals provided by RFID reader 104. For example, in one exemplary embodiment, fob 102 may include a 134 KHz antenna 218 configured to communicate with a 134 KHz transponder 220. In this exemplary configuration, an ISO/IEC 14443-2 compliant modulator/demodulator may not be required. Instead, the 134 KHz transponder may be configured to communicate directly with the protocol/sequence controller 208 for transmission and receipt of authentication and account number signals as described above.

In another embodiment, fob 102 may further include a universal serial bus (USB) connector 132 for interfacing fob 102 to a user interface 134. User interface 134 may be further in communication with a POS device 110 via a network 136. Network 136 may be the Internet, an intranet, or the like as is described above with respect to network 112. Further, the user interface 134 may be similar in construction to any conventional input devices and/or computing systems aforementioned for permitting the system user to interact with the system. In one exemplary embodiment, fob 102 may be configured to facilitate online Internet payments. A USB converter 222 may be in communication with a USB connector 232 for facilitating the transfer of information between the modulator/demodulator 206 and USB connector 132. Alternatively, USB converter 222 may be in communication with protocol/sequence controller 208 to facilitate the transfer of information between protocol/sequence controller 208 and USB connector 132.

Where fob 102 includes a USB connector 132, fob 102 may be in communication with, for example, a USB port on user interface 134. The information retrieved from fob 102 may be compatible with credit card and/or smart card technology enabling usage of interactive applications on the Internet. No RFID reader may be required in this embodiment since the connection to POS device 110 may be made using a USB port on user interface 134 and a network 136.

Fob 102 may include means for enabling activation of the fob by the user. In one exemplary embodiment, a switch 230 which may be operated by the user of the fob 102. The switch 230 on fob 102 may be used to selectively or inclusively activate the fob 102 for particular uses. In this context, the term "selectively" may mean that the switch 230 enables the user to place the fob 102 in a particular

operational mode. For example, the user may place the fob 102 in a mode for enabling purchase of a good or of a service using a selected account number. Alternatively, the fob may be placed in a mode as such that the fob account number is provided by USB port 132 (or serial port) only and the fob transponder 114 is disabled. In addition, the term "inclusively" may mean that the fob 102 is placed in an operational mode permitting the fob 102 to be responsive to the RF interrogation and interrogation via the USB connector 132. In one particular embodiment, the switch 230 may remain in an OFF position ensuring that one or more applications or accounts associated with the fob 102 are non-reactive to any commands issued by RFID reader 104. As used herein, the OFF position may be termed the "normal" position of the activation switch 230, although other normal positions are contemplated.

In another exemplary embodiment, when the switch 230 is moved from the OFF position, the fob 102 may be deemed activated by the user. That is, the switch 230 may activate internal circuitry in fob 102 for permitting the fob to be responsive to RF signals (*e.g.*, commands from RFID reader 104). In this way, switch 230 may facilitate control of the active and inactive states of the fob 102. Such control increases the system security by preventing inadvertent or illegal use of the fob 102.

In one exemplary embodiment, switch 230 may be a simple mechanical device in communication with circuitry which may electrically prevent the fob from being powered by a RFID reader. That is, when switch 230 is in its normal position, switch 230 may provide a short to the fob 102 internal circuitry, preventing fob 102 from being responsive to interrogation by RF or via the USB connector 230. In this arrangement, the switch 230 may be, for example, a "normally closed" (NC) configured switch, which may be electrically connected to the antenna 202 at the interface of the antenna 202 and the transponder 114. The switch 230 may be depressed, which may open the switch 230 fully activating the antenna 202.

In yet another exemplary embodiment, the fob 102 may include a biometric sensor and biometric membrane configured to operate as switch 230 and activate the fob 102 when provided biometric signal from the fob 102 user. Such biometric signal may be the digital reading of a fingerprint, thumbprint, or the like. Typically, where biometric circuitry is used, the biometric circuitry may be powered by an internal voltage source (*e.g.*, battery). In this case, the switch may not be a simple

mechanical device, but a switch which is powered. In yet another exemplary embodiment, switch 230 may be battery powered though no biometric circuitry is present in the fob 102.

In yet another embodiment, the switch 230 may be a logic switch. Where switch 230 is a logic switch the switch 230 control software may be read from the sequence controller 208 to selectively control the activation of the various fob 102 components.

FIG. 3 illustrates an exemplary block diagram of a RFID reader 104 in accordance with an exemplary embodiment of the present invention. RFID reader 104 includes, for example, an antenna 106 coupled to a RF module 302, which is further coupled to a control module 304. In addition, RFID reader 104 may include an antenna 108 positioned remotely from the RFID reader 104 and coupled to RFID reader 104 via a suitable cable 120, or other wire or wireless connection.

RF module 302 and antenna 106 may be suitably configured to facilitate communication with fob 102. Where fob 102 is formatted to receive a signal at a particular RF frequency, RF module 302 may be configured to provide an interrogation signal at that same frequency. For example, in one exemplary embodiment, fob 102 may be configured to respond to an interrogation signal of about 13.56 MHz. In this case, RFID antenna 106 may be 13 MHz and may be configured to transmit an interrogation signal of about 13.56 MHz. That is, fob 102 may be configured to include a first and second RF module (*e.g.*, transponder) where the first module may operate using a 134 kHz frequency and the second RF module may operate using a 13.56 MHz frequency. The RFID reader 104 may include two receivers which may operate using the 134 kHz frequency, the 13.56 MHz frequency or both. When the reader 104 is operating at 134 kHz frequency, only operation with the 134 kHz module on the fob 102 may be possible. When the reader 104 is operating at the 13.56 MHz frequency, only operation with the 13.56 MHz module on the fob 102 may be possible. Where the reader 104 supports both a 134 kHz frequency and a 13.56 MHz RF module, the fob 102 may receive both signals from the reader 104. In this case, the fob 102 may be configured to prioritize selection of the one or the other frequency and reject the remaining frequency. Alternatively, the reader 104 may receive signals at both frequencies from the fob

upon interrogation. In this case, the reader 104 may be configured to prioritize selection of one or the other frequency and reject the remaining frequency.

Further, protocol/sequence controller 314 may include an optional feedback function for notifying the user of the status of a particular transaction. For example, the optional feedback may be in the form of an LED, LED screen and/or other visual display which is configured to light up or display a static, scrolling, flashing and/or other message and/or signal to inform the fob 102 user that the transaction is initiated (*e.g.*, fob is being interrogated), the fob is valid (*e.g.*, fob is authenticated), transaction is being processed, (*e.g.*, fob account number is being read by RFID reader) and/or the transaction is accepted or denied (*e.g.*, transaction approved or disapproved). Such an optional feedback may or may not be accompanied by an audible indicator (or may present the audible indicator singly) for informing the fob 102 user of the transaction status. The audible feedback may be a simple tone, multiple tones, musical indicator, and/or voice indicator configured to signify when the fob 102 is being interrogated, the transaction status, or the like.

RFID antenna 106 may be in communication with a transponder 306 for transmitting an interrogation signal and receiving at least one of an authentication request signal and/or an account data from fob 102. Transponder 306 may be of similar description as transponder 114 of FIG. 2. In particular, transponder 306 may be configured to send and/or receive RF signals in a format compatible with antenna 202 in similar manner as was described with respect to fob transponder 114. For example, where transponder 306 is 13.56 MHz RF rated antenna 202 may be 13.56 MHz compatible. Similarly, where transponder 306 is ISO/IEC 14443 rated, antenna 106 may be ISO/IEC 14443 compatible.

RF module 302 may include, for example, transponder 306 in communication with authentication circuitry 308 which may be in communication with a secure database 310. Authentication circuitry 308 and database 310 may be of similar description and operation as described with respect to authentication circuitry 210 and secure memory database 212 of FIG. 2. For example, database 310 may store data corresponding to the fob 102 which are authorized to transact business over system 100. Database 310 may additionally store RFID reader 104 identifying information for providing to fob 102 for use in authenticating whether RFID reader

104 is authorized to be provided the fob account number stored on fob database 214.

Authentication circuitry 308 may be of similar description and operation as authentication circuitry 210. That is, authentication circuitry 308 may be configured to authenticate the signal provided by fob 102 in similar manner that authentication circuitry 210 may be configured to authenticate the signal provided by RFID reader 104. As is described more fully below, fob 102 and RFID reader 104 engage in mutual authentication. In this context, "mutual authentication" may mean that operation of the system 100 may not take place until fob 102 authenticates the signal from RFID reader 104, and RFID reader 104 authenticates the signal from fob 102.

Fig. 4 is a flowchart of an exemplary authentication process in accordance with the present invention. The authentication process is depicted as one-sided. That is, the flowchart depicts the process of the RFID reader 104 authenticating the fob 102, although similar steps may be followed in the instance that fob 102 authenticates RFID reader 104.

As noted, database 212 may store security keys for encrypting or decrypting signals received from RFID reader 104. In an exemplary authentication process, where RFID reader 104 is authenticating fob 102, RFID reader 104 may provide an interrogation signal to fob 102 (step 402). The interrogation signal may include a random code generated by the RFID reader authentication circuit 210, which is provided to the fob 102 and which is encrypted using an unique encryption key corresponding to the fob 102 unique identification code. For example, the protocol/sequence controller 314 may provide a command to activate the authentication circuitry 308. Authentication circuitry 308 may provide from database 310 a fob interrogation signal including a random number as a part of the authentication code generated for each authentication signal. The authentication code may be an alphanumeric code which is recognizable (*e.g.*, readable) by the RFID reader 104 and the fob 102. The authentication code may be provided to the fob 102 via the RFID RF interface 306 and antenna 106 (or alternatively antenna 108).

Fob 102 receives the interrogation signal (step 404). The interrogation signal including the authorization code may be received at the RF interface 114 via

antenna 202. Once the fob 102 is activated, the interrogation signal including the authorization code may be provided to the modulator/demodulator circuit 206 where the signal may be demodulated prior to providing the signal to protocol/sequence controller 208. Protocol/sequence controller 208 may recognize the interrogation signal as a request for authentication of the fob 102, and provide the authentication code to authentication circuit 210. The fob 102 may then encrypt the authentication code (step 406). In particular, encryption may be done by authentication circuit 210, which may receive the authentication code and encrypt the code prior to providing the encrypted authentication code to protocol/sequence controller 208. Fob 102 may then provide the encrypted authentication code to the RFID reader 104 (step 408). That is, the encrypted authentication code may be provided to the RFID reader 104 via modulator/demodulator circuit 206, RF interface 114 (*e.g.*, transponder 114) and antenna 202.

RFID reader 104 may then receive the encrypted authentication code and decryption it (step 410). That is, the encrypted authentication code may be received at antenna 106 and RF interface 306 and may be provided to authentication circuit 308. Authentication circuit 308 may be provided a security authentication key (*e.g.*, transponder system decryption key) from database 310. The authentication circuit may use the authentication key to decrypt (*e.g.*, unlock) the encrypted authorization code. The authentication key may be provided to the authentication circuit based on the fob 102 unique identification code. For example, the encrypted authentication code may be provided along with the unique fob 102 identification code. The authentication circuit may receive the fob 102 unique identification code and retrieve from the database 310 a transponder system decryption key correlative to the unique fob 102 identification code for use in decrypting the encrypted authentication code.

Once the authentication code is decrypted, the decrypted authentication code is compared to the authentication code provided by the RFID reader 104 at step 402 (step 412) to verify its authenticity. If the decrypted authorization code is not readable (*e.g.*, recognizable) by the authentication circuit 308, the fob 102 is deemed to be unauthorized (*e.g.*, unverified) (step 416) and the operation of system 100 is terminated (step 418). Contrarily, if the decrypted authorization code is recognizable (*e.g.*, verified) by the fob 102, the decrypted authorization code is

deemed to be authenticated (step 412), and the transaction is allowed to proceed (step 414). In one particular embodiment, the proceeding transaction may mean that the fob 102 may authenticate the RFID reader 104, although, it should be apparent that the RFID reader 104 may authenticate the fob 102 prior to the fob 102 authenticating the RFID reader 104.

It should be noted that in an exemplary verification process, the authorization circuit 308 may determine whether the unlocked authorization code is identical to the authorization code provided in step 402. If the codes are not identical then the fob 102 is not authorized to access system 100. Although, the verification process is described with respect to identicality, identicality is not required. For example, authentication circuit 308 may verify the decrypted code through any protocol, steps, or process for determining whether the decrypted code corresponds to an authorized fob 102.

Authentication circuitry 308 may additionally be in communication with a protocol/sequence controller 314 of similar operation and description as protocol/sequence controller 208 of FIG. 2. That is, protocol/sequence device controller 314 may be configured to determine the order of operation of the RFID reader 104 components. For example, FIG. 5 illustrates and exemplary decision process under which protocol/sequence controller 314 may operate. Protocol/sequence controller 314 may command the different components of RFID reader 104 based on whether a fob 102 is present (step 502). For example, if a fob 102 is not present, then protocol/sequence controller 314 may command the RFID reader 104 to provide an uninterrupted interrogation signal (step 504). That is, the protocol/sequence controller may command the authentication circuit 308 to provide an uninterrupted interrogation signal until the presence of a fob 102 is realized. If a fob 102 is present, the protocol/sequence controller 314 may command the RFID reader 104 to authenticate the fob 102 (step 506).

As noted above, authentication may mean that the protocol/sequence controller 314 may command the authentication circuit 308 to provide fob 102 with an authorization code. If a response is received from fob 102, protocol/sequence controller may determine if the response is a response to the RFID reader 104 provided authentication code, or if the response is a signal requiring authentication (step 508). If the signal requires authentication, then the protocol/sequence

controller 314 may activate the authentication circuit as described above (step 506). On the other hand, if the fob 102 signal is a response to the provided authentication code, then the protocol/sequence controller 314 may command the RFID reader 104 to retrieve the appropriate security key for enabling recognition of the signal (step 510). That is, the protocol/sequence controller 314 may command the authentication circuit 308 to retrieve from database 310 a security key (*e.g.*, transponder system decryption key), unlock the signal, and compare the signal to the signal provided by the RFID reader 104 in the authentication process (*e.g.*, step 506). If the signal is recognized, the protocol/sequence controller 314 may determine that the fob 102 is authorized to access the system 100. If the signal is not recognized, then the fob is considered not authorized. In which case, the protocol/sequence controller 314 may command the RFID controller to interrogate for authorized fobs (step 504).

Once the protocol/sequence controller determines that the fob 102 is authorized, the protocol/sequence controller 314 may seek to determine if additional signals are being sent by fob 102 (step 514). If no additional signal is provided by fob 102, then the protocol/sequence controller 314 may provide all the components of RFID reader 104 to remain idle until such time as a signal is provided (step 516). Contrarily, where an additional fob 102 signal is provided, the protocol/sequence controller 314 may determine if the fob 102 is requesting access to the merchant point of sale terminal 110 (*e.g.*, POS device) or if the fob 102 is attempting to interrogate the RFID reader 104 for return (*e.g.*, mutual) authorization (step 518). Where the fob 102 is requesting access to a merchant point of sale terminal 110, the protocol/sequence controller 314 may command the RFID reader to open communications with the point of sale terminal 110 (step 524). In particular, the protocol/sequence controller may command the point of sale terminal communications interface 312 to become active, permitting transfer of data between the RFID reader 104 and the merchant point of sale terminal 110.

On the other hand, if the protocol/sequence controller determines that the fob 102 signal is a mutual interrogation signal, then the protocol/sequence controller may command the RFID reader 104 to encrypt the signal (step 520). The protocol/sequence controller 314 may command the encryption authentication circuit 318 to retrieve from database 320 the appropriate encryption key in response to the

fob 102 mutual interrogation signal. The protocol/sequence controller 314 may then command the RFID reader 104 to provide the encrypted mutual interrogation signal to the fob 102. The protocol/sequence controller 314 may command the authentication circuit 318 to provide an encrypted mutual interrogation signal for the fob 102 to mutually authenticate. Fob 102 may then receive the encrypted mutual interrogation signal and retrieve from authentication circuitry 212 a RFID reader decryption key.

Although an exemplary decision process of protocol/sequence controller 314 is described, it should be understood that a similar decision process may be undertaken by protocol/sequence controller 208 in controlling the components of fob 102. Indeed, as described above, protocol/sequence controller 314 may have similar operation and design as protocol/sequence controller 208. In addition, to the above, protocol/sequence controllers 208 and 314 may incorporate in the decision process appropriate commands for enabling USB interfaces 222 and 316, when the corresponding device is so connected.

Encryption/decryption component 318 may be further in communication with a secure account number database 320 which stores the security keys necessary for decrypting the encrypted fob account number. Upon appropriate request from protocol/sequence controller 314, encryption/decryption component (*e.g.*, circuitry 318) may retrieve the appropriate security key, decrypt the fob account number and forward the decrypted account number to protocol sequence controller 314 in any format readable by any later connected POS device 110. In one exemplary embodiment, the account number may be forwarded in a conventional magnetic stripe format compatible with the ISO/IEC 7813 standard. Upon receiving the account number in magnetic stripe format, protocol/sequence controller 314 may forward the account number to POS device 110 via a communications interface 312 and data link 122, as best shown in Figure 1. POS device 110 may receive the decrypted account number and forward the magnetic stripe formatted account number to a merchant network 112 for processing under the merchant's business as usual standard. In this way, the present invention eliminates the need of a third-party server. Further, where the POS device 110 receives a response from network 112 (*e.g.*, transaction authorized or denied), protocol/sequence controller 314 may

provide the network response to the RF module 302 for optically and/or audibly communicating the response to the fob 102 user.

RFID reader 104 may additionally include a USB interface 316, in communication with the protocol/sequence controller 314. In one embodiment, the USB interface may be a RS22 serial data interface. Alternatively, the RFID reader 104 may include a serial interface such as, for example, a RS232 interface in communication with the protocol/sequence controller 314. The USB connector 316 may be in communication with a personalization system 116 (shown in FIG. 1B) for initializing RFID reader 104 to system 100 application parameters. That is, prior to operation of system 100, RFID reader 104 may be in communication with personalization system 116 for populating database 310 with a listing of security keys belonging to authorized fobs 102, and for populating database 320 with the security keys to decrypt the fob 102 account numbers placing the account numbers in ISO/IEC 7813 format. In this way, RFID reader 104 may be populated with a unique identifier (*e.g.*, serial number) which may be used by fob authentication circuitry 210 to determine if RFID reader 104 is authorized to receive a fob 102 encrypted account number.

FIG. 1B illustrates an exemplary personalization system 100B, in accordance with the present invention. In general, typical personalization system 100B may be any system for initializing the RFID reader 104 and fob 102 for use in system 100A. With reference to FIG. 1B, the similar personalization process for fob 102 may be illustrated. For example, personalization system 116 may be in communication with fob 102 via RF ISO 14443 interface 114 for populating fob database 212 with the security keys for facilitating authentication of the unique RFID reader 104 identifier. In addition, personalization system 116 may populate on database 212 a unique fob 102 identifier for use by RFID reader 104 in determining whether fob 102 is authorized to access system 100. Personalization system 116 may populate (*e.g.*, inject) the encrypted fob 102 account number into fob database 214 for later providing to an authenticated RFID reader 104.

In one exemplary embodiment, personalization system 116 may include any standard computing system as described above. For example, personalization system 116 may include a standard personal computer containing a hardware security module operable using any conventional graphic user interface. Prior to

populating the security key information account number and unique identifying information into the fob 102 or RFID reader 104, the hardware security module may authenticate the fob 102 and RFID reader 104 to verify that the components are authorized to receive the secure information.

FIGS. 6A-B illustrate an exemplary flowchart of a personalization procedure which may be used to personalize fob 102 and/or RFID reader 104. Although the following description discusses mainly personalization of fob 102, RFID reader 104 may be personalized using a similar process. The personalization process, which occurs between the personalization system 116 and the device to be personalized (*e.g.*, fob 102 or RFID reader 104), may begin, for example at step 602. Mutual authentication may occur between the personalization system 116 and the device to be authenticated in much the same manner as was described above with regard to fob 102 mutually authenticating with RFID reader 104. That is, personalization system 116 may transmit a personalization system 116 identifier to the device to be authenticated which is compared by the device authentication circuitry 210, 308 against personalization system identifiers stored in the device database 212, 310. Where a match does not occur (step 604), the personalization process may be aborted (step 612). Where a match occurs (step 604), the personalization system may prepare a personalization file to be provided to the device to be personalized (step 606). If the personalization system is operated manually, the personalization file may be entered into the personalization system 116 using any suitable system interface such as, for example, a keyboard (step 606). Where the personalization system 116 operator elects to delay the preparation of the personalization files, the system 116 may abort the personalization process (step 610). In this context, the personalization file may include the unique fob 102 or RFID reader 104 identifier, security key for loading into database 212 and 310, and/or security keys for decrypting a fob account number which may be loaded in database 320.

Fob 102 may be personalized by direct connection to the personalization system 116 via RF ISO/IEC 14443 interface 114, or the fob 102 may be personalized using RFID reader 104. Personalization system 116 and RFID reader 104 may engage in mutual authentication and RFID reader 104 may be configured to transmit the fob personalization file to fob 102 via RF. Once the fob 102 is presented to RFID reader 104 (steps 608, 614) for personalization, fob 102 and

RFID reader 104 may engage in mutual authentication (step 614). Where the fob 102 is not presented to the RFID reader 104 for personalization, the personalization process may be aborted (step 610).

If the fob 102 is detected, the personalization system 116 may create as a part of the personalization file, a unique identifier for providing to the fob 102 (step 616). The identifier is unique in that one identifier may be given only to a single fob. That is, no other fob may have that same identifier. The fob may then be configured and loaded with that identifier (step 618).

The encrypted fob 102 account number may be populated into fob 102 in the same manner as is described with respect to the fob 102 unique identifier. That is, personalization system 116 may pre-encrypt the account data (step 640) and inject the encrypted account into fob database 214 (step 622). The encrypted account data may be loaded (*e.g.*, injected) into the fob 102 using RFID reader 104 as discussed above.

Once the personalization file is populated into the fob 102, the populated information is irreversibly locked to prevent alteration, unauthorized reading and/or unauthorized access (step 624). Personalization system 116 may then create a log of the personalization file information for later access and analysis by the personalization system 116 user (step 626).

It should be noted that in the event the personalization system 116 process is compromised or interrupted (step 628), the personalization system may send a security alert to the user (step 630) and the personalization process may be aborted (step 612). On the other hand, where no such compromising or interruption exists, the personalization system may be prepared to begin initialization on a second device to be personalized (step 632).

FIGS. 7A-B illustrate another exemplary embodiment of a personalization process which may be used to personalize RFID reader 104. RFID reader 104 may be in communication with a personalization system 116 via RFID reader USB connection 316 (step 702). Once connected, personalization system 116 may establish communications with the RFID reader 104 and RFID reader 104 may provide personalization system 116 any RFID reader 104 identification data presently stored on the RFID reader 104 (step 704). In accordance with step 708, where the RFID reader 104 is being personalized for the first time (step 706) the

RFID reader 104 and the personalization system 116 may engage in mutual authentication as described above with respect to FIGS. 6A-B. After the mutual authentication is complete, personalization system 116 may verify that RFID reader 104 is properly manufactured or configured to operate within system 100. The verification may include evaluating the operation of the RFID reader 104 by determining if the RFID reader will accept predetermined default settings. That is, the personalization system 116 may then provide the RFID reader 104 a set of default settings (step 708) and determine if the RFID reader 104 accepts those settings (step 712). If RFID reader 104 does not accept the default settings, personalization system 116 may abort the personalization process (step 714).

If the personalization system 116 determines that the personalization process is not the first personalization process undertaken by the RFID reader 104 (step 706), personalization system 116 and RFID reader 104 may engage in a mutual authentication process using the existing security keys already stored on RFID reader 104 (step 710). If authentication is unsuccessful (step 712), the personalization system may abort the personalization process (step 714).

Where the personalization system 116 and the RFID reader 104 successfully mutually authenticate, the personalization system 116 may update the RFID reader 104 security keys (step 716). Updating the security keys may take place at any time as determined by a system 100 manager. The updating may take place as part of a routine maintenance or merely to install current security key data. The updating may be performed by downloading firmware into RFID reader 104 (step 718). In the event that the personalization system determines in step 706 that the RFID reader 104 is undergoing an initial personalization, the firmware may be loaded into the RFID reader 104 for the first time. In this context, "firmware" may include any file which enables the RFID reader 102 to operate under system 100 guidelines. For example, such guidelines may be directed toward the operation of RFID reader protocol/sequence controller 314.

Personalization system 116 may then determine if the personalization keys (*e.g.*, security keys, decryption keys, RFID identifier) need to be updated or if the RFID reader 104 needs to have an initial installation of the personalization keys (step 720). If so, then personalization system 116 may download the personalization keys as appropriate (step 722).

Personalization system 116 may then check the RFID reader 104 to determine if the fob 102 identifiers and corresponding security keys should be updated or initially loaded (step 724). If no updating is necessary the personalization system may end the personalization procedure (step 732). Contrarily, if the personalization system 116 determines that the fob 102 identifiers and corresponding keys need to be updated or installed, the personalization system may download the information onto RFID reader 104 (step 726). The information (*e.g.*, fob security keys and identifiers) may be downloaded in an encrypted format and the RFID reader 104 may store the information in the RFID reader database 310 as appropriate (step 728). The personalization system may then create or update a status log cataloging for later use and analysis by the personalization system 116 user (step 730). Upon updating the status log, the personalization process may be terminated (step 732).

It should be noted that, in some instances it may be necessary to repersonalize the RFID reader in similar manner as described above. In that instance, the personalization method described in FIGS. 7A and 7B may be repeated.

FIG. 8 illustrates an exemplary flow diagram for the operation of system 100A. The operation may be understood with reference to FIG. 1A, which depicts the elements of system 100A which may be used in an exemplary transaction. The process is initiated when a customer desires to present a fob 102 for payment (step 802). Upon presentation of the fob 102, the merchant initiates the RF payment procedure via an RFID reader 104 (step 804). In particular, the RFID reader sends out an interrogation signal to scan for the presence of fob 102 (step 806). The RF signal may be provided via the RFID reader antenna 106 or optionally via an external antenna 108. The customer then may present the fob 102 for payment (step 808) and the fob 102 is activated by the RF interrogation signal provided.

The fob 102 and the RFID reader 104 may then engage in mutual authentication (step 810). Where the mutual authentication is unsuccessful, an error message may be provided to the customer via the RFID optical and/or audible indicator (step 814) and the transaction may be aborted (step 816). Where the mutual authentication is successful (step 814), the RFID reader 104 may provide the customer with an appropriate optical and/or audible message (*e.g.*, "transaction

processing" or "wait") (step 818). The fob protocol/sequence controller 208 may then retrieve from database 214 an encrypted fob account number and provide the encrypted account number to the RFID reader 104 (step 820).

The RFID reader 104 may then decrypt the account number and convert the account number into magnetic stripe (ISO/IEC 7813) format (step 822) and provide the unencrypted account number to the merchant system 130 (step 828). In particular, the account number may be provided to the POS 110 device for transmission to the merchant network 112 for processing under known business transaction standards. The POS device 110 may then send an optical and/or audible transaction status message to the RFID reader 104 (step 830) for communication to the customer (step 832).

It should be noted that the transaction account associated with the fob 102 may include a restriction, such as, for example, a per purchase spending limit, a time of day use, a day of week use, certain merchant use and/or the like, wherein an additional verification is required when using the fob outside of the restriction. The restrictions may be personally assigned by the fob 102 user, or the account provider. For example, in one exemplary embodiment, the account may be established such that purchases above $X (*i.e.*, the spending limit) must be verified by the customer. Such verification may be provided using a suitable personal identification number (PIN) which may be recognized by the RFID reader 104 or a payment authorization center (not shown) as being unique to the fob 102 holder (*e.g.*, customer) and the correlative fob 102 transaction account number. Where the requested purchase is above the established per purchase spending limit, the customer may be required to provide, for example, a PIN, biometric sample and/or similar secondary verification to complete the transaction.

Where a verification PIN is used as secondary verification the verification PIN may be checked for accuracy against a corroborating PIN which correlates to the fob 102 transaction account number. The corroborating PIN may be stored locally (*e.g.*, on the fob 102, or on the RFID reader 104) or may be stored on a database (not shown) at the payment authorization center. The payment authorization center database may be any database maintained and operated by the fob 102 transaction account provider.

The verification PIN may be provided to the POS device 110 using a conventional merchant (*e.g.*, POS) PIN key pad 118 in communication with the POS device 110 as shown in FIG. 1, or a RFID keypad in communication with the RFID reader 104. PIN keypad may be in communication with the POS device 110 (or alternatively, RFID reader 104) using any conventional data link described above. Upon receiving the verification PIN, the RFID reader 104 may seek to match the PIN to the corroborating PIN stored on the RFID reader 104 at database 310 or 320. Alternatively, the verification PIN may be provided to a payment authorization center to determine whether the PIN matches the PIN stored on the payment authorization center database which correlates to the fob 102 account. If a match is made, the purchase may no longer be restricted, and the transaction may be allowed to be completed.

In an alternate embodiment, verification of purchases exceeding the established spending limit may involve biometrics circuitry included in fob 102. FIG. 9 is a schematic block diagram of an exemplary fob 102 wherein fob 102 includes a biometric security system 902. Biometric security system 902 may include a biometric sensor 904 for sensing the fingerprint of the fob 102 user. The biometric sensor 902 may be in communication with a sensor interface/driver 906 for receiving the sensor fingerprint and activating the operation of fob 102. In communication with the biometric sensor 904 and sensor interface 906 may be a battery 903 for providing the necessary power for operation of the biometric security system components.

In one exemplary application of the fob 102 including the biometric security system 902, the customer may place his finger on the biometric sensor to initiate the mutual authentication process between the fob 102 and the RFID reader 104, or to provide secondary verification of the user's identity. The sensor fingerprint may be digitized and compared against a digitized fingerprint stored in a database (*e.g.*, security database 212) included on fob 102. Such comparison step may be controlled by protocol/sequence controller 208 and may be validated by authentication circuit 210. Where such verification is made, the mutual authentication between fob 102 and RFID reader 104 may begin, and the transaction may proceed accordingly. Alternatively, the comparison may be made with a digitized fingerprint stored on a database maintained by the fob 102

transaction account provider system (not shown). The digitized fingerprint may be verified in much the same way as is described above with respect to the PIN.

In one exemplary application of the fob 102 including the biometric security system 902, the system 902 may be used to authorize a purchase exceeding the established per purchase spending limit. In this case, where the customer's intended purchase exceeds the spending limit, the customer may be asked to provide assurance that the purchase is authorized. Accordingly, the customer may provide such verification by placing his finger over the biometric sensor 904. The biometric sensor 904 may then digitize the fingerprint and provide the digitized fingerprint for verification as described above. Once verified, fob 102 may provide a transaction authorized signal to RF transponder 202 (or alternatively to transponder 220) for forwarding to RFID reader 104. RFID reader 104 may then provide the transaction authorized signal to the POS device 110 in similar manner as is done with convention PIN driven systems and the POS device 110 may process the transaction under the merchant's business as usual standard.

The preceding detailed description of exemplary embodiments of the invention makes reference to the accompanying drawings, which show the exemplary embodiment by way of illustration. While these exemplary embodiments are described in sufficient detail to enable those skilled in the art to practice the invention, it should be understood that other embodiments may be realized and that logical and mechanical changes may be made without departing from the spirit and scope of the invention. Thus, the preceding detailed description is presented for purposes of illustration only and not of limitation, and the scope of the invention is defined solely by the appended claims and their legal equivalents when properly read in light of the preceding description. For example, the steps recited in any of the method or process claims may be executed in any order and are not limited to the order presented.

Claims

We claim:

1. A transponder-reader payment system comprising:

a. a Radio Frequency Identification (RFID) reader operable to provide a radio frequency (RF) interrogation signal for powering a transponder system, receiving a transponder system RF signal, and communicating a transponder system account data related to said transponder system RF signal to a merchant system, said RFID reader including,

i. a first interrogator for providing a first RF interrogation signal;

ii. a RFID authentication circuit in communication with said interrogator;

iii. a RFID database, in communication with said RFID authentication circuit;

iv. a universal serial bus (USB) interface; and

v. a RFID protocol/sequence controller in communication with at least one of said first interrogator, said RFID authentication circuit, said RFID database, and said USB interface, said RFID protocol/sequence controller configured to facilitate control of the order of operation of said interrogator, said RFID authentication circuit, said RFID database, and said USB interface.

2. A system according to claim 1 further comprising:

a. a transponder system operable to receive said first RF interrogation signal, authenticate said first RF interrogation signal, and transmit said transponder system account data, said transponder system comprising a

i. a first transponder responsive to said RF interrogation signal;

ii. a second transponder responsive to a second RF interrogation signal, said first RF interrogation signal different from said second RF interrogation signal;

iii. a transponder system authentication circuit in communication with at least one of said first transponder and said second transponder; and

iv. a transponder system database in communication with said transponder system authentication circuit.

3. A system according to claim 2, wherein said transponder system further includes:

a. a transponder system USB interface; and

b. a transponder system protocol/sequence controller in communication with at least one of said first transponder, said second transponder, said transponder system USB interface, said transponder system authentication circuit, and said transponder system database, said transponder system protocol/sequence controller configured to control the order of operation of said first transponder, said second transponder, said transponder system authentication circuit, said transponder system database, and said transponder system USB interface.

4. A system according to claim 1, wherein said RFID reader further includes:

a. a second interrogator, said second interrogator operable to send a second RF interrogation signal; and

b. a RFID communications interface configured to communicate with a merchant system, said communications interface operable to provide said transponder system account data.

5. A system according to claim 4, wherein said RFID reader further includes a first antenna in communication with said first interrogator and a second antenna in communication with said second interrogator, wherein said first antenna is operable to provide said first RF interrogation signal to said first transponder and said second interrogator is operable to provide said second RF interrogation signal to said second transponder.

6. A system according to claim 1, wherein said RFID reader further comprises at least one of a universal serial bus (USB) and a serial interface.

7. A system according to claim 1, wherein said RFID database is operable to store at least one of a RFID reader identifying data, a transponder system

decryption security key, a RFID reader encryption security key, an transponder authentication key and a transponder system personal identification number (PIN).

8. A system according to claim 5, wherein said RFID reader further comprises at least one of a RFID internal antenna, and a RFID external antenna, said RFID internal antenna and said RFID external antenna configured to provide at least one of said first RF interrogation signal and said second RF interrogation signal.

9. A system according to claim 2, wherein said transponder system further comprises at least one of a first transponder system antenna and a second transponder system antenna, said first transponder system antenna configured to receive said first RF interrogation signal, and said second transponder system antenna configured to receive said second RF interrogation signal.

10. A system according to claim 3, wherein said transponder system protocol/sequence controller is responsive to at least one of said first RF interrogation signal and said second RF interrogation signal, said transponder protocol/sequence controller controlling the sequence of operation at least one of said transponder system authentication circuit, said transponder system database, and said transponder system USB interface in response to at least one of said first RF interrogation signal and said second RF interrogation signal.

11. A system according to claim 3, wherein said transponder system protocol/sequence controller is configured to activate said transponder system authentication circuit in response to said first RF interrogation signal, said transponder system authenticating circuit configured to provide an encrypted RF interrogation signal, said transponder system authentication circuit configured to provide said encrypted RF interrogation signal to said first transponder for providing to said RFID reader.

12. A system according to claim 11, wherein said RFID reader is configured to receive said encrypted RF interrogation signal, said transponder system

protocol/sequence controller activating said transponder system authentication circuit in response to said encrypted RF interrogation signal.

13. A system according to claim 12, wherein said RFID database is configured to provide a transponder system decryption key to said RFID authentication circuit in response to said encrypted RF interrogation signal, said transponder system decryption key for use in decrypting said encrypted RF interrogation signal, providing a decrypted RF interrogation signal, said transponder system decryption key provided to said reader based on an unique transponder identification code.

14. A system according to claim 13, wherein said RFID authentication circuit is configured to compare said decrypted RF interrogation signal and said RF interrogation signal to determine whether a match exists.

15. A system according to claim 14, wherein said RFID protocol/sequence controller is configured to activate at least one of said USB interface and said RFID communication interface where said RFID authentication circuit matches said decrypted RF interrogation signal and said RF interrogation signal.

16. A system according to claim 15, wherein said transponder system protocol/sequence controller activates said transponder system authentication circuit in response to at least one of said first RF interrogation signal and said second RF interrogation signal.

17. A claim according to claim 16, wherein said transponder system authentication circuit is configured to provide a transponder authentication code to at least one of said first transponder and said second transponder for providing to said RFID reader.

18. A system according to claim 17, wherein said RFID reader is configured to receive said transponder authentication code, said RFID protocol/sequence controller activating said RFID authentication circuit in response to said transponder

authentication code, said RFID authentication circuit configure to encrypt said transponder authentication code.

19. A system according to claim 18, wherein said RFID reader is configured to provide said encrypted authentication code to said transponder system.

20. A system according to claim 19, wherein said transponder system database is operable to store at least one of a transponder system identification data, a RFID reader decryption security key, a transponder system account data.

21. A system according to claim 20, wherein said transponder system database is configured to provide said RFID reader decryption security key to said transponder system authentication circuit in response to said encrypted authentication code, said RFID reader decryption key for use in decrypting said encrypted transponder authentication code, providing a decrypted transponder authentication code.

22. A system according to claim 21, wherein said transponder system authentication circuit is configured to compare said decrypted transponder authentication code and said transponder authentication code to determine if a match exists.

23. A system according to claim 22, wherein said account data is in magnetic stripe format.

24. A system according to claim 23, wherein said transponder system transaction account data is pre-encrypted.

25. A system according to claim 24, wherein said transponder system database is configured to provide said pre-encrypted transponder system account data to said RFID reader where said transponder system authentication circuit matches said decrypted transponder authentication code and said transponder authentication code.

26. A system according to claim 25, wherein said RFID communications interface is configured to provide said transponder system PIN and said pre-encrypted transponder system account data where said transponder authentication code matches said decrypted transponder authentication code, and said decrypted RF interrogation signal matches said RF interrogation signal.

27. A system according to claim 26, wherein said transponder system further comprises a switch, said switch operable to enable or disable operation of said transponder system.

28. A system according to claim 27, wherein said switch is configured to place the transponder system in at least one of a selectivity mode and an inclusivity mode.

29. A system according to claim 27, wherein said switch is mechanical.

30. A system according to claim 27, wherein said switch is configured to respond to a logic circuit.

31. A system according to claim 2, wherein said transponder system further includes an internal power source.

32. A system according to claim 31, wherein said switch is in communication with said internal power source, said switch responsive to said internal power source.

33. A system according to claim 31, wherein said transponder system further includes a biometric circuit, said biometric circuit in communication with said internal power source.

34. A system according to claim 27, wherein said switch is a biometric circuit, said biometric circuit operable to enable or disenable operation of said transponder system.

35. A system according to claim 34, wherein said biometric circuit is configured to place said transponder system in one of a selectivity mode and an inclusivity mode.

36. A system according to claim 7, wherein said RFID reader includes a RFID PIN keypad, said RFID PIN keypad configured to receive said transponder PIN, said RFID reader configured to compare said transponder PIN to said received transponder PIN, said RFID reader operable to provide at least one of said received transponder PIN, said transponder PIN, or a verification of said received transponder PIN, verification of received transponder PIN provided where said RFID reader matches said transponder PIN to said received transponder PIN.

37. A system according to claim 7, wherein said RFID reader is configured to provide said transponder PIN to a payment authorization center for verification of said transponder PIN.

38. A system according to claim 36, wherein said merchant system includes a merchant system PIN keypad, said merchant system PIN keypad configured to receive said transponder PIN from said merchant system PIN keypad, said merchant system configured to provide said transponder PIN to said payment authorization center for verification.

39. A system according to claim 33, wherein said biometric circuit is configured to provide a biometric data verification response, said biometric circuit configured to provide said biometric data verification response to at least one of said RFID reader and said merchant system, wherein said biometric data verification response is an identification verification data.

40. A system according to claim 3, further comprising a personalization system operable to initialize at least one of said transponder system and said RFID reader to transponder-reader payment system parameters.

41. A system according to claim 40, wherein said personalization system is in RF communications with said transponder system using at least one of a USB connector and RF communications.

42. A system according to claim 41, wherein said personalization system is in electrical communications with said RFID reader.

43. A system according to claim 42, wherein said personalization system is operable to populate at least one of said RFID reader identifying data, transponder system decryption security key, RFID encryption security key, and transponder PIN on said RFID database.

44. A system according to claim 43, wherein said personalization system is operable to populate at least one of said transponder system identification data, a RFID reader decryption security key, a transponder encryption authentication security key, a transponder system transactional account data, and a transponder system authentication security key onto said transponder system database.

45. A system according to claim 2, wherein said RFID reader is operable to initialize said transponder.

46. A system according to claim 2, wherein said RFID reader is in RF communication with said transponder system, said RFID reader operable to populate at least one of said transponder system identification data, a RFID reader decryption security key, a transponder system transactional account data onto said transponder system database.

47. A transponder-reader payment system comprising:

a transponder system operable to receive a first RF interrogation signal, and authenticate said first RF interrogation signal, said transponder system comprising:

a. a first transponder responsive to said first RF interrogation signal; and

b. a second transponder responsive to a second RF interrogation signal, said first RF interrogation signal different from said second RF interrogation signal.

48. A system according to claim 47, wherein said transponder system further includes a transponder system USB interface.

49. A system according to claim 47, wherein said transponder system further includes a serial interface.

50. A transponder-reader payment system comprising

a transponder system operable to receive a first RF interrogation signal, and authenticate said first RF interrogation signal, said transponder system comprising a transponder system USB interface.

51. A transponder-reader payment system comprising a RFID reader operable to provide at least a first interrogator for providing a first interrogation signal and a second interrogator for providing a second interrogation signal.

52. A method of transponder-reader payment comprising the steps of:

a. providing a transponder system, the transponder system responsive to a plurality of interrogation signals, the transponder system storing at least one of an account data, an account name, and account expiration date; and

b. providing a RFID reader, said reader configured to provide at least one of the interrogation signals.

53. A method according to claim 52, further comprising the steps of:

a. encrypting the transponder system account data;

b. initializing the transponder system;

c. initializing the RFID reader;

d. mutually authenticating the RFID reader and the transponder system;

e. providing the encrypted account data from the transponder system to the RFID reader;

f. decrypting the encrypted account data; and

g. providing the decrypted account data to a merchant system.

54. A method according to claim 53, wherein mutual authenticating includes the RFID reader authenticating the transponder system, and the transponder system authenticating the RFID reader.

55. A method according to claim 54, wherein mutual authentication includes:

a. providing an interrogation signal from the RFID reader to the transponder system;

b. encrypting the interrogation signal at the transponder system to form an encrypted authentication interrogation signal;

c. providing the encrypted authentication interrogation signal to the RFID reader;

d. decrypting the encrypted authentication interrogation signal at the RFID reader, decrypting including using a transponder system decryption security key;

e. matching the interrogation signal to the decrypted interrogation signal;

f. providing an authorization code from the transponder system to the RFID reader;

g. encrypting the authorization code at the RFID reader to form an encrypted authorization code;

h. providing the encrypted authorization code to the transponder system;

i. decrypting the encrypted authorization code at the transponder system, decrypting including using a RFID reader decryption security key;

j. matching the authorization code to the decrypted authorization code.

56. A method according to 55, where initializing the transponder system includes populating at least one of a transponder system identification data, a RFID reader decryption security key, a transponder system transactional data, and an encrypted transponder PIN onto a transponder system database.

57. A method according to claim 56, wherein initializing the RFID reader includes populating at least one of a RFID reader identifying data, a transponder system decryption security key, a RFID encryption security key, and a transponder PIN onto a RFID database.

58. A method according to claim 52, wherein initializing the RFID reader includes populating at least one of a RFID reader identifying data, a transponder system decryption security key, a RFID encryption key, and a transponder PIN onto a RFID database using a USB interface.

59. A method according to claim 56, wherein initializing the transponder system includes populating at least one of a transponder system identification date, a RFID reader decryption security key, and a transponder system transaction data using a USB interface.

60. A method according to claim 52, wherein initialing the transponder system, includes initializing said transponder system using a RFID reader.

61. A method according to claim 57, including using a switch to enable the transponder system, the switch consisting of at least one of a mechanical switch, a logic switch, and a biometric switch.

62. A method according to claim 61, including providing a secondary identification in response to a request from a merchant system.

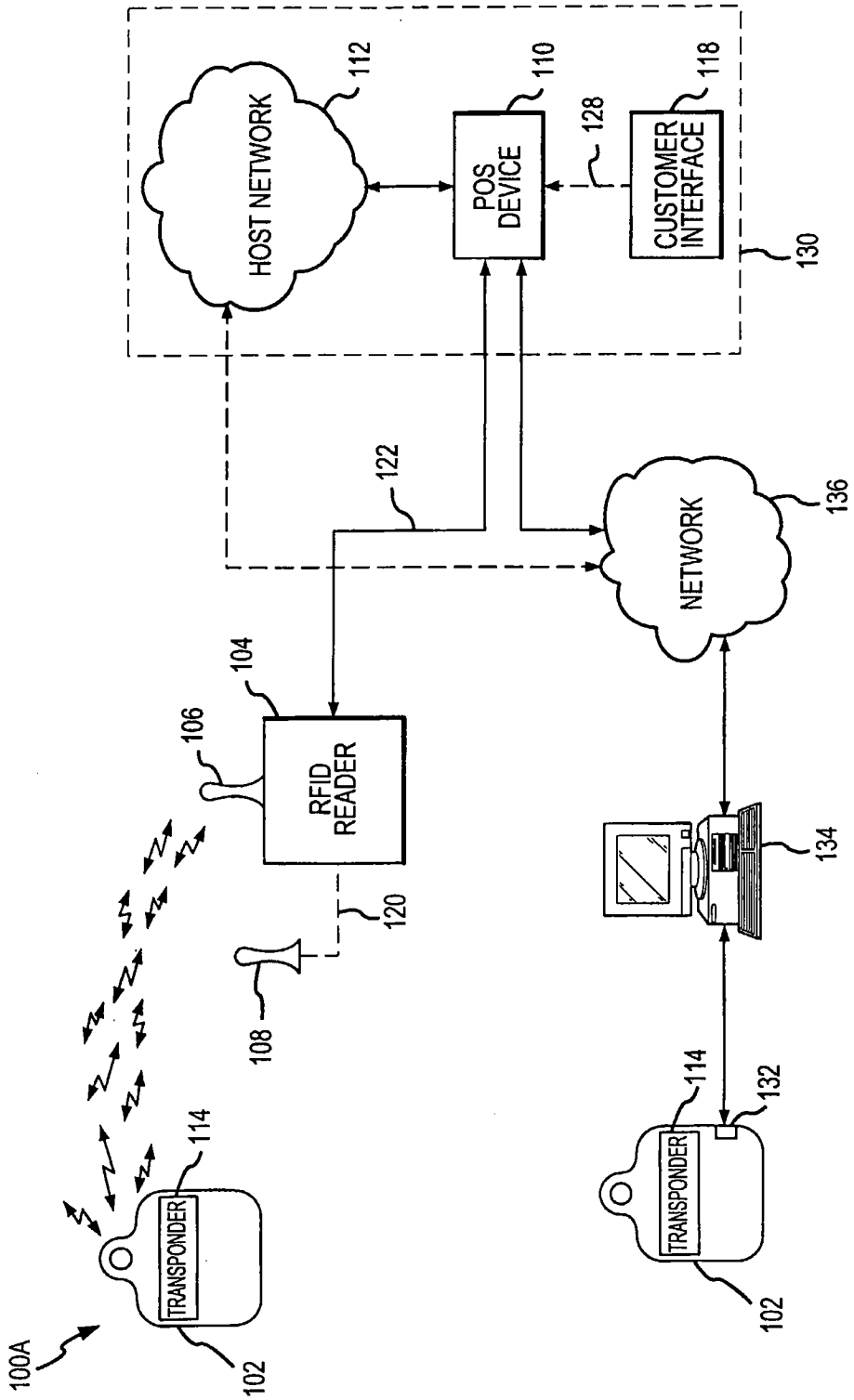

HOST NETWORK
112
POS DEVICE
110
128
CUSTOMER INTERFACE
118
130
122
NETWORK
136
104
106
RFID READER
120
108
134
114
132
TRANSPONDER
102
100A

FIG.1A

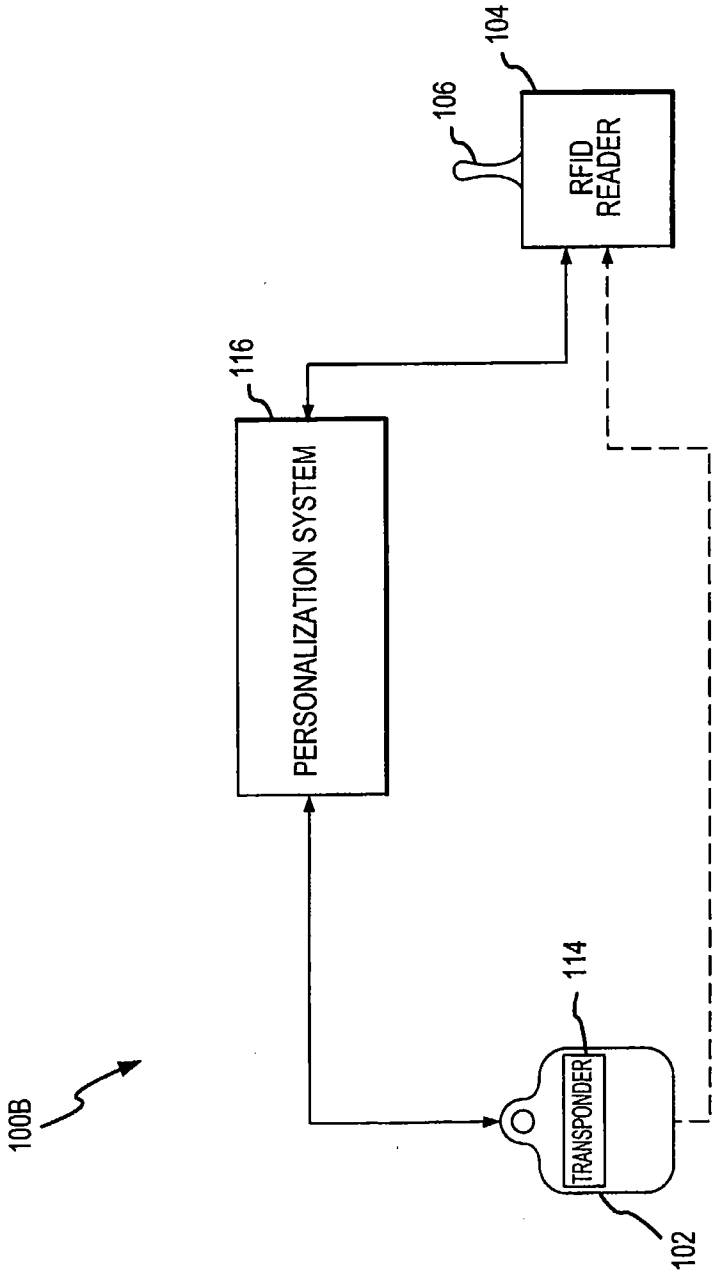

100B
102
TRANSPONDER
114
PERSONALIZATION SYSTEM
116
RFID READER
106
104

FIG.1B

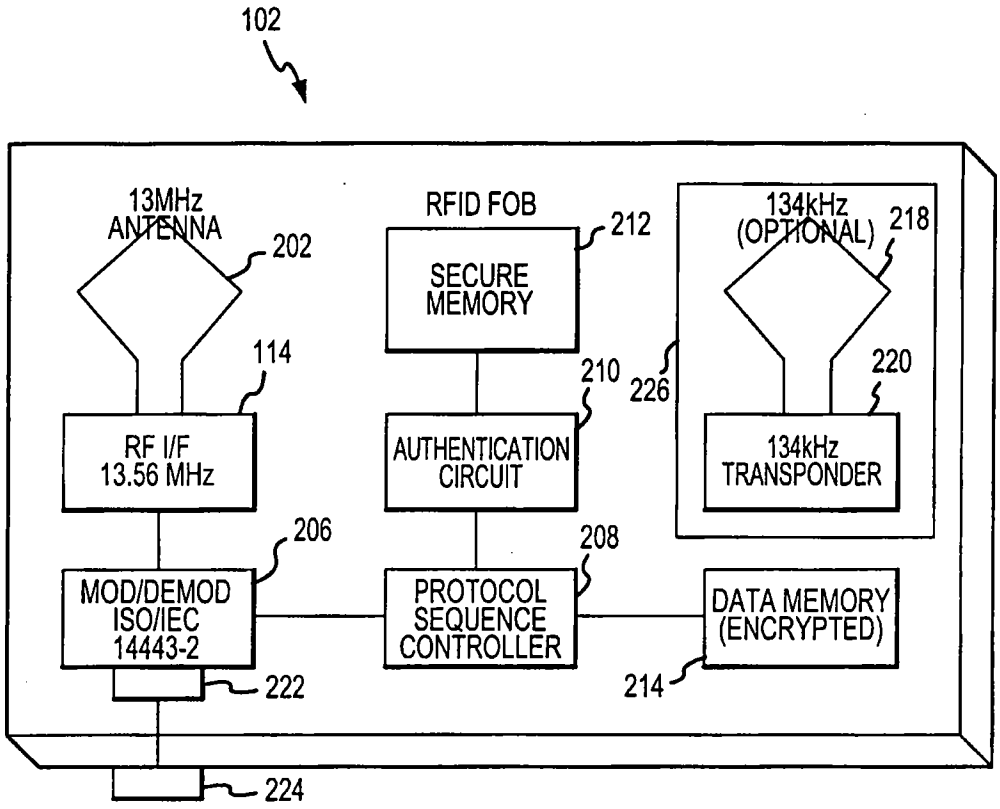

102
13MHz ANTENNA
202
114
RF I/F 13.56 MHz
206
MOD/DEMOD ISO/IEC 14443-2
222
224
RFID FOB
212
SECURE MEMORY
210
AUTHENTICATION CIRCUIT
208
PROTOCOL SEQUENCE CONTROLLER
214
DATA MEMORY (ENCRYPTED)
226
134kHz (OPTIONAL)
218
220
134kHz TRANSPONDER

FIG.2

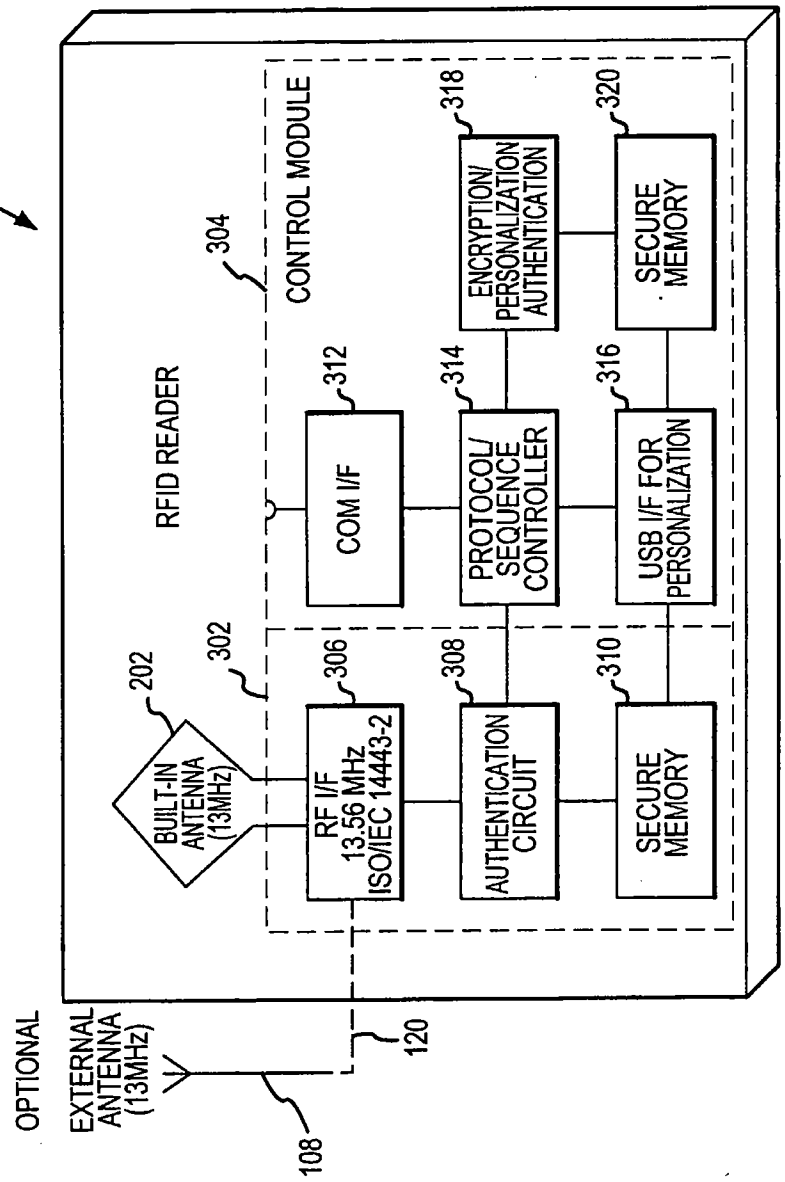

104
RFID READER
CONTROL MODULE
304
318
320
ENCRYPTION/ PERSONALIZATION AUTHENTICATION
SECURE MEMORY
312
314
316
COM I/F
PROTOCOL/ SEQUENCE CONTROLLER
USB I/F FOR PERSONALIZATION
202
302
306
308
310
BUILT-IN ANTENNA (13MHz)
RF I/F 13.56 MHz ISO/IEC 14443-2
AUTHENTICATION CIRCUIT
SECURE MEMORY
OPTIONAL
EXTERNAL ANTENNA (13MHz)
120
108

FIG.3

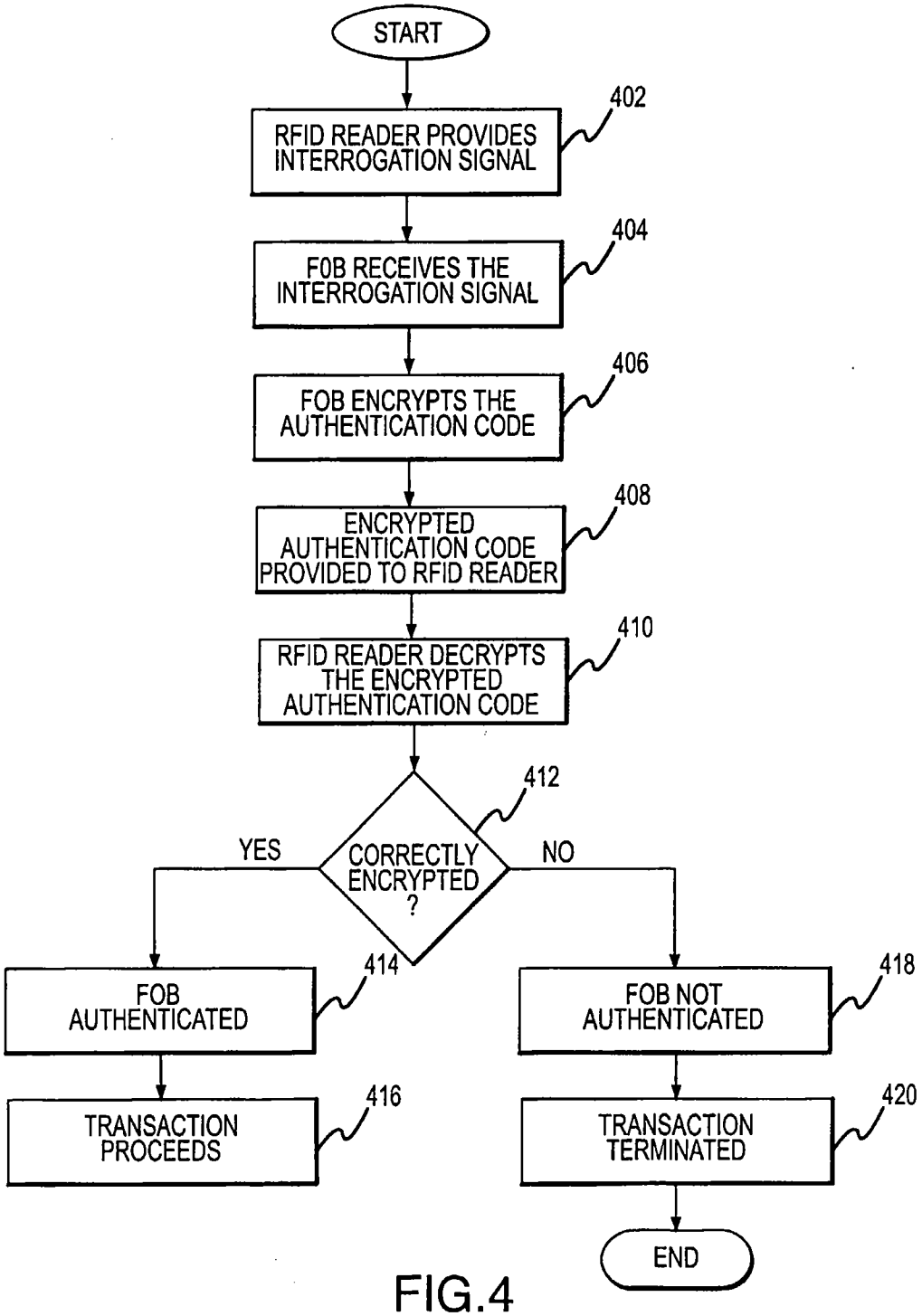

START
RFID READER PROVIDES INTERROGATION SIGNAL
402
FOB RECEIVES THE INTERROGATION SIGNAL
404
FOB ENCRYPTS THE AUTHENTICATION CODE
406
ENCRYPTED AUTHENTICATION CODE PROVIDED TO RFID READER
408
RFID READER DECRYPTS THE ENCRYPTED AUTHENTICATION CODE
410
CORRECTLY ENCRYPTED ?
412
YES
NO
FOB AUTHENTICATED
414
FOB NOT AUTHENTICATED
418
TRANSACTION PROCEEDS
416
TRANSACTION TERMINATED
420
END

FIG.4

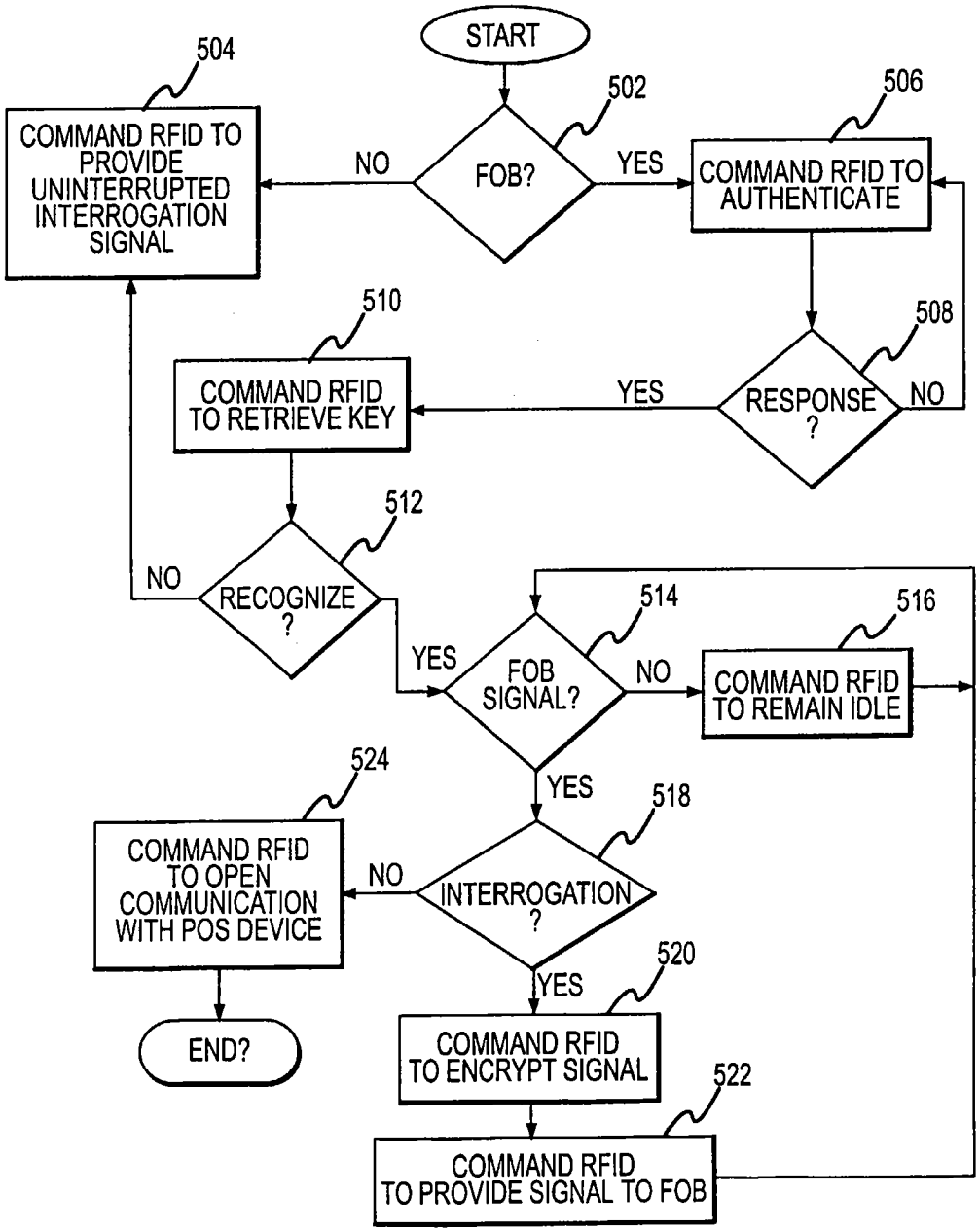

START
502
FOB?
NO
YES
504
COMMAND RFID TO PROVIDE UNINTERRUPTED INTERROGATION SIGNAL
506
COMMAND RFID TO AUTHENTICATE
508
RESPONSE ?
YES
NO
510
COMMAND RFID TO RETRIEVE KEY
512
RECOGNIZE ?
NO
YES
514
FOB SIGNAL?
NO
516
COMMAND RFID TO REMAIN IDLE
YES
518
INTERROGATION ?
NO
524
COMMAND RFID TO OPEN COMMUNICATION WITH POS DEVICE
YES
520
COMMAND RFID TO ENCRYPT SIGNAL
522
COMMAND RFID TO PROVIDE SIGNAL TO FOB
END?

FIG.5

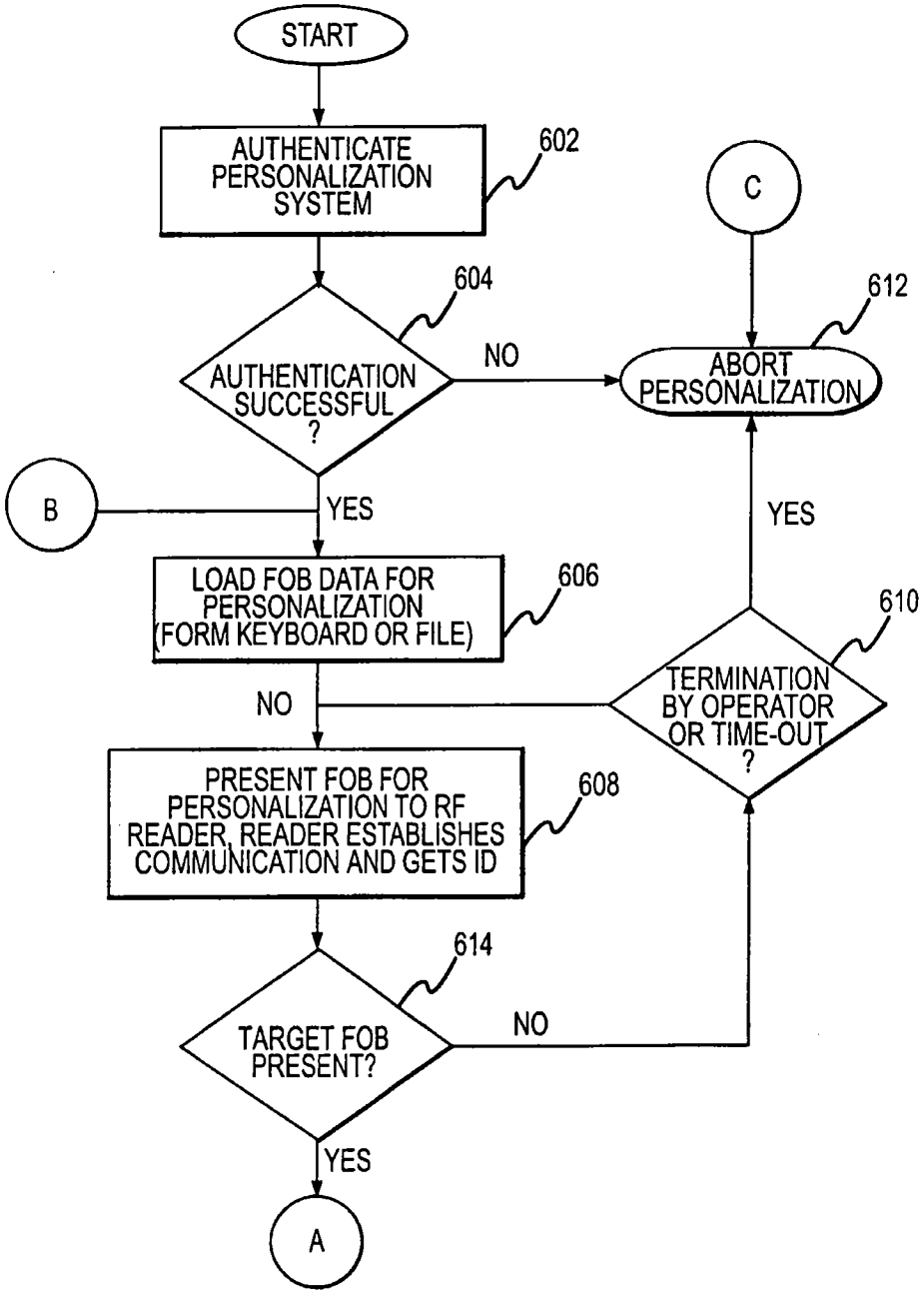

START
AUTHENTICATE PERSONALIZATION SYSTEM
602
AUTHENTICATION SUCCESSFUL ?
604
NO
ABORT PERSONALIZATION
612
C
B
YES
YES
LOAD FOB DATA FOR PERSONALIZATION (FORM KEYBOARD OR FILE)
606
TERMINATION BY OPERATOR OR TIME-OUT ?
610
NO
PRESENT FOB FOR PERSONALIZATION TO RF READER, READER ESTABLISHES COMMUNICATION AND GETS ID
608
TARGET FOB PRESENT?
614
NO
YES
A

FIG.6A

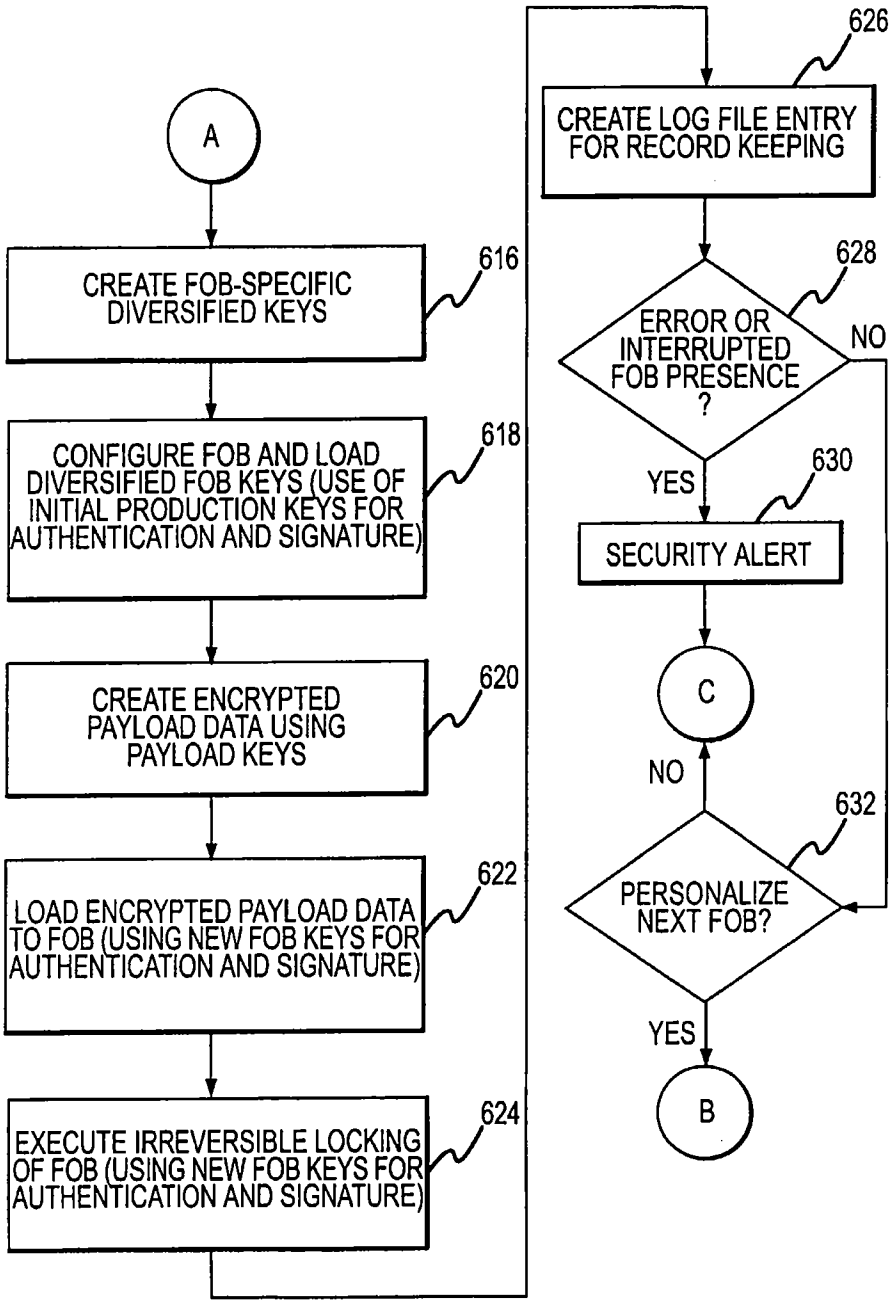

A
CREATE FOB-SPECIFIC DIVERSIFIED KEYS
616
CONFIGURE FOB AND LOAD DIVERSIFIED FOB KEYS (USE OF INITIAL PRODUCTION KEYS FOR AUTHENTICATION AND SIGNATURE)
618
CREATE ENCRYPTED PAYLOAD DATA USING PAYLOAD KEYS
620
LOAD ENCRYPTED PAYLOAD DATA TO FOB (USING NEW FOB KEYS FOR AUTHENTICATION AND SIGNATURE)
622
EXECUTE IRREVERSIBLE LOCKING OF FOB (USING NEW FOB KEYS FOR AUTHENTICATION AND SIGNATURE)
624
626
CREATE LOG FILE ENTRY FOR RECORD KEEPING
628
ERROR OR INTERRUPTED FOB PRESENCE ?
NO
YES
630
SECURITY ALERT
C
NO
632
PERSONALIZE NEXT FOB?
YES
B

FIG.6B

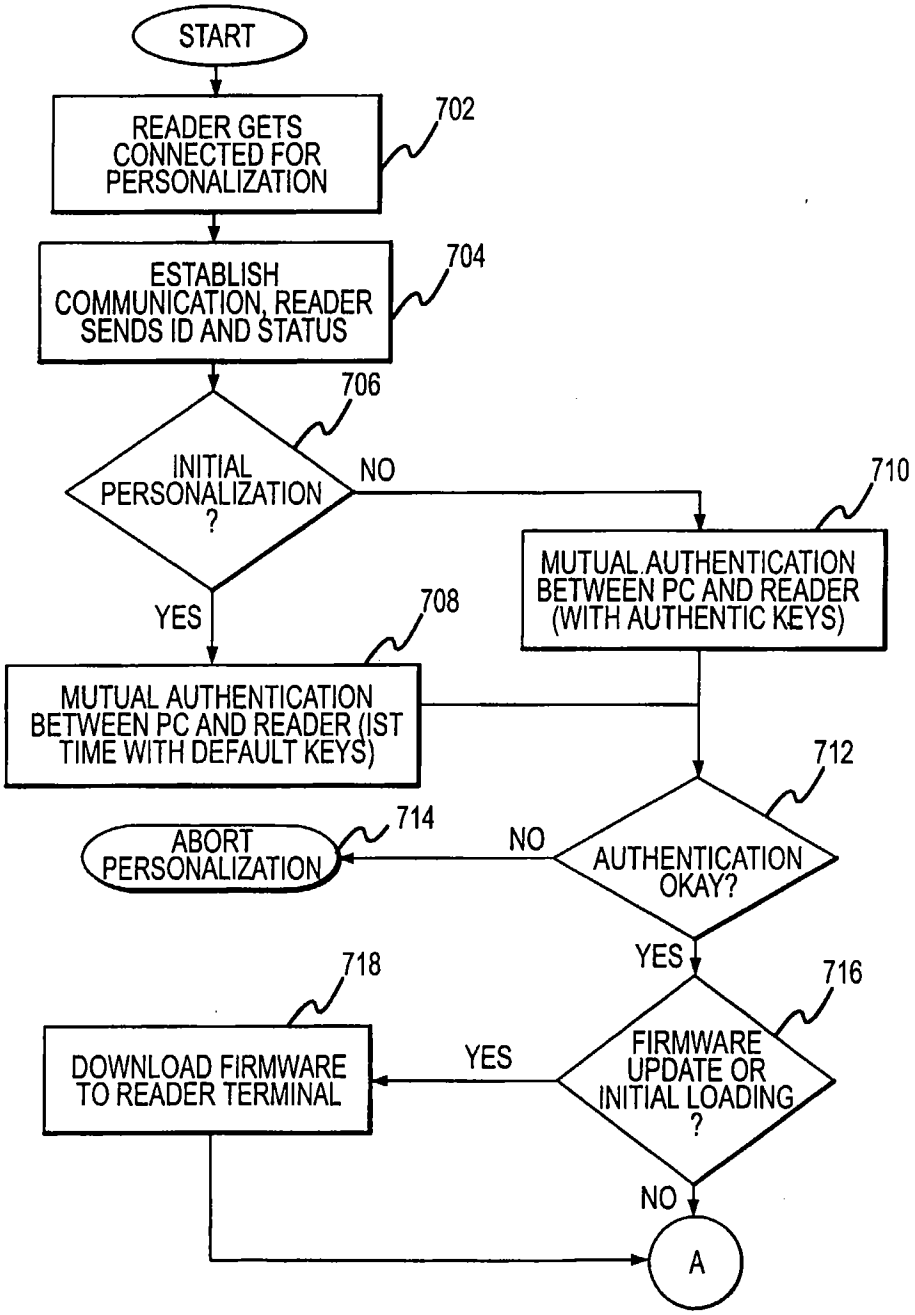

START
READER GETS CONNECTED FOR PERSONALIZATION
702
ESTABLISH COMMUNICATION, READER SENDS ID AND STATUS
704
706
INITIAL PERSONALIZATION ?
NO
710
MUTUAL AUTHENTICATION BETWEEN PC AND READER (WITH AUTHENTIC KEYS)
YES
708
MUTUAL AUTHENTICATION BETWEEN PC AND READER (IST TIME WITH DEFAULT KEYS)
712
ABORT PERSONALIZATION
714
NO
AUTHENTICATION OKAY?
YES
718
716
DOWNLOAD FIRMWARE TO READER TERMINAL
YES
FIRMWARE UPDATE OR INITIAL LOADING ?
NO
A

FIG.7A

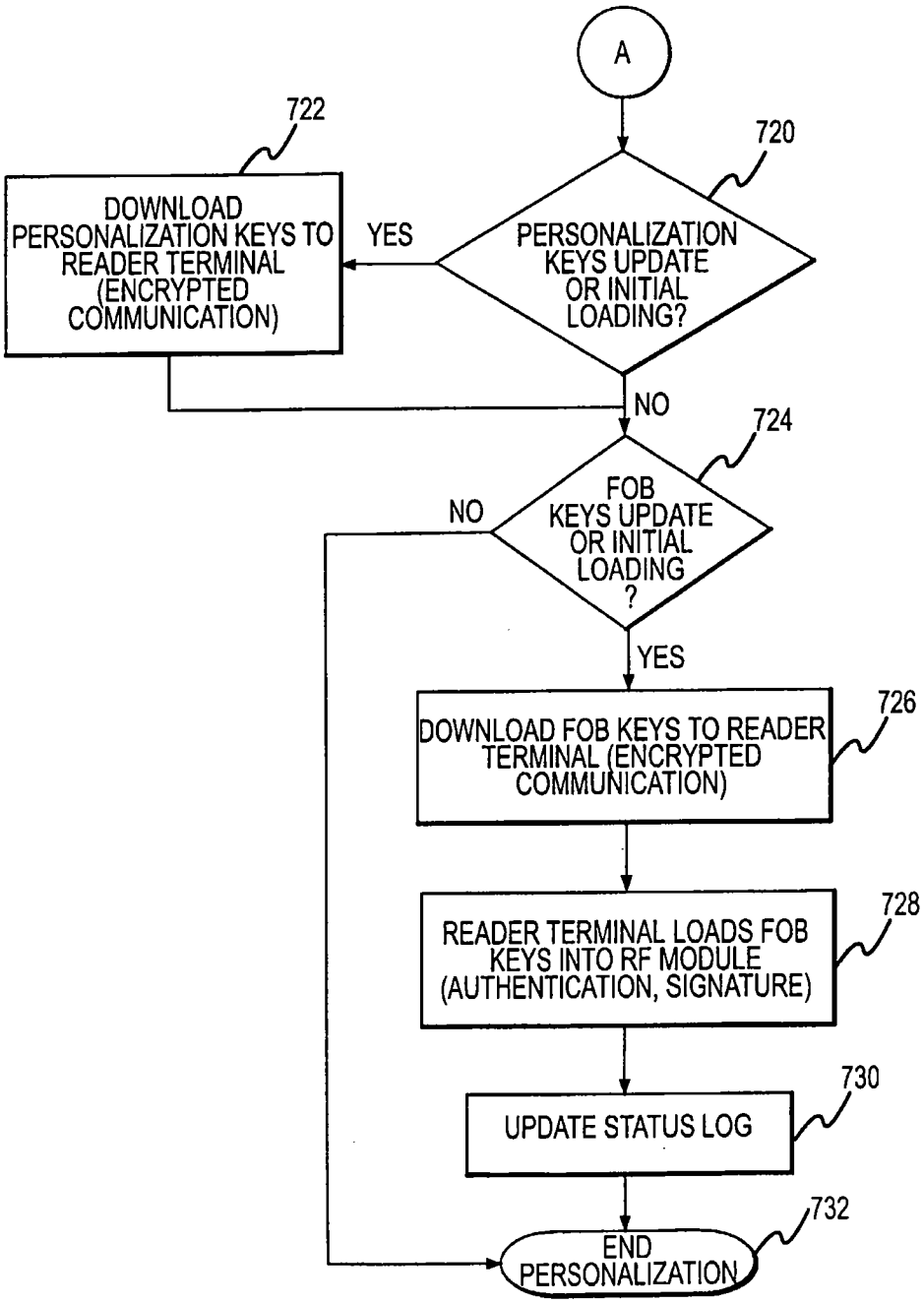

A
722
720
DOWNLOAD PERSONALIZATION KEYS TO READER TERMINAL (ENCRYPTED COMMUNICATION)
YES
PERSONALIZATION KEYS UPDATE OR INITIAL LOADING?
NO
724
NO
FOB KEYS UPDATE OR INITIAL LOADING ?
YES
726
DOWNLOAD FOB KEYS TO READER TERMINAL (ENCRYPTED COMMUNICATION)
728
READER TERMINAL LOADS FOB KEYS INTO RF MODULE (AUTHENTICATION, SIGNATURE)
730
UPDATE STATUS LOG
732
END PERSONALIZATION

FIG.7B

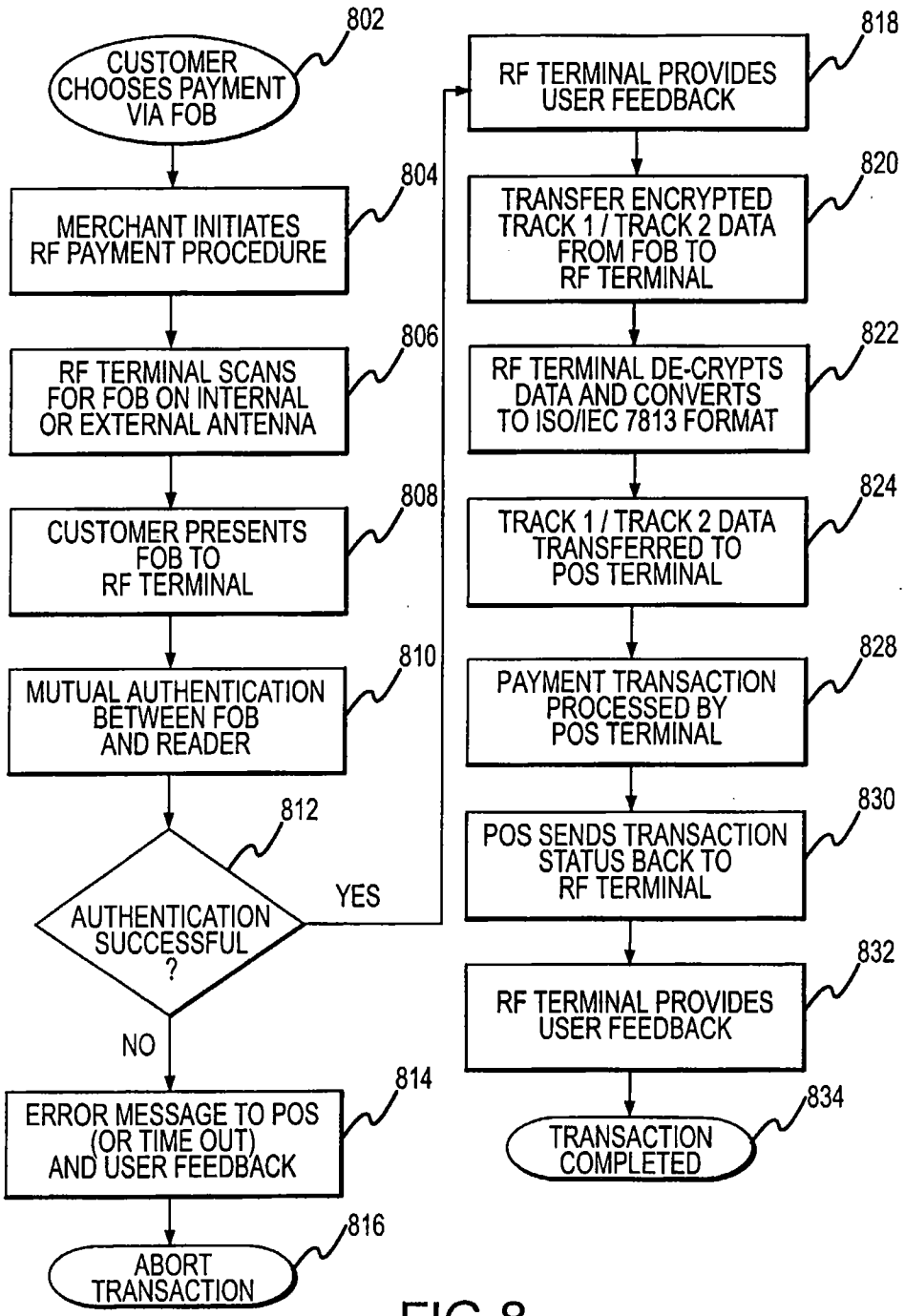

802
CUSTOMER CHOOSES PAYMENT VIA FOB
804
MERCHANT INITIATES RF PAYMENT PROCEDURE
806
RF TERMINAL SCANS FOR FOB ON INTERNAL OR EXTERNAL ANTENNA
808
CUSTOMER PRESENTS FOB TO RF TERMINAL
810
MUTUAL AUTHENTICATION BETWEEN FOB AND READER
812
AUTHENTICATION SUCCESSFUL ?
YES
NO
814
ERROR MESSAGE TO POS (OR TIME OUT) AND USER FEEDBACK
816
ABORT TRANSACTION
818
RF TERMINAL PROVIDES USER FEEDBACK
820
TRANSFER ENCRYPTED TRACK 1 / TRACK 2 DATA FROM FOB TO RF TERMINAL
822
RF TERMINAL DE-CRYPTS DATA AND CONVERTS TO ISO/IEC 7813 FORMAT
824
TRACK 1 / TRACK 2 DATA TRANSFERRED TO POS TERMINAL
828
PAYMENT TRANSACTION PROCESSED BY POS TERMINAL
830
POS SENDS TRANSACTION STATUS BACK TO RF TERMINAL
832
RF TERMINAL PROVIDES USER FEEDBACK
834
TRANSACTION COMPLETED

FIG.8

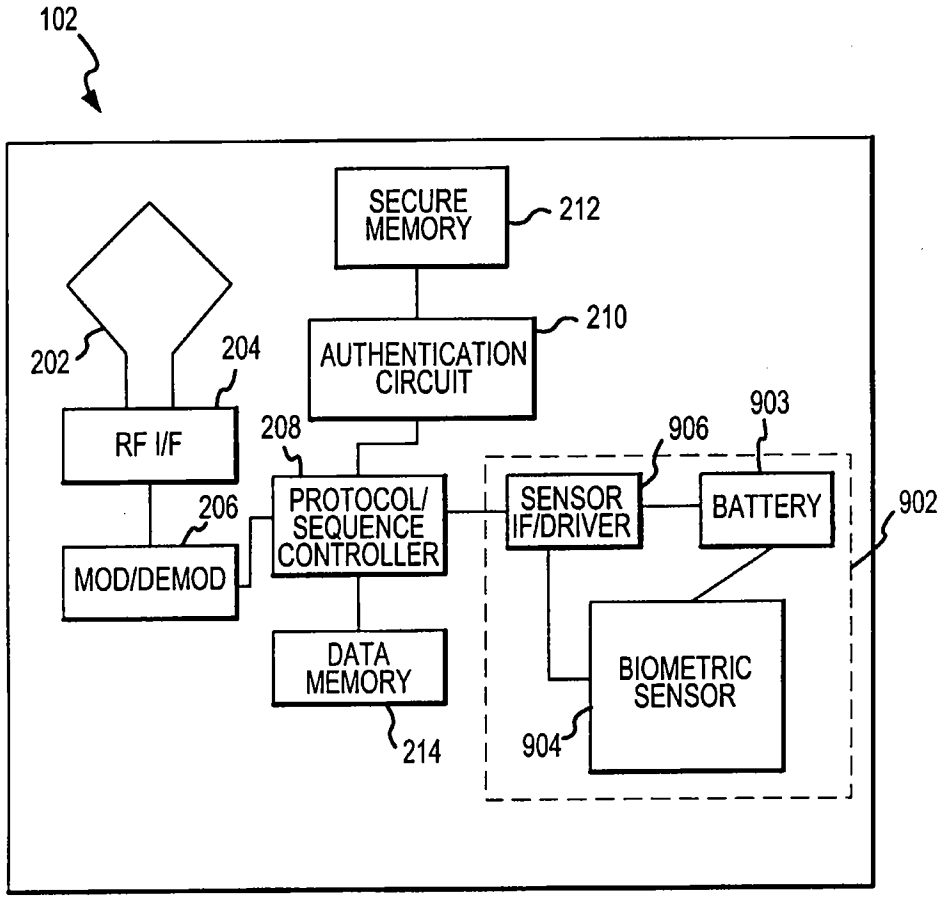

102
SECURE MEMORY
212
AUTHENTICATION CIRCUIT
210
202
204
RF I/F
208
903
906
206
PROTOCOL/ SEQUENCE CONTROLLER
SENSOR IF/DRIVER
BATTERY
902
MOD/DEMOD
DATA MEMORY
214
BIOMETRIC SENSOR
904

FIG.9

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007623 A3

(51) International Patent Classification[7]: H04Q 1/00, G05B 19/00

(21) International Application Number: PCT/US02/21903

(22) International Filing Date: 10 July 2002 (10.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/304,216 10 July 2001 (10.07.2001) US

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPAGNY, INC [US/US]; American Express Tower, World Financial Center, New York, NY 10285-4900 (US).

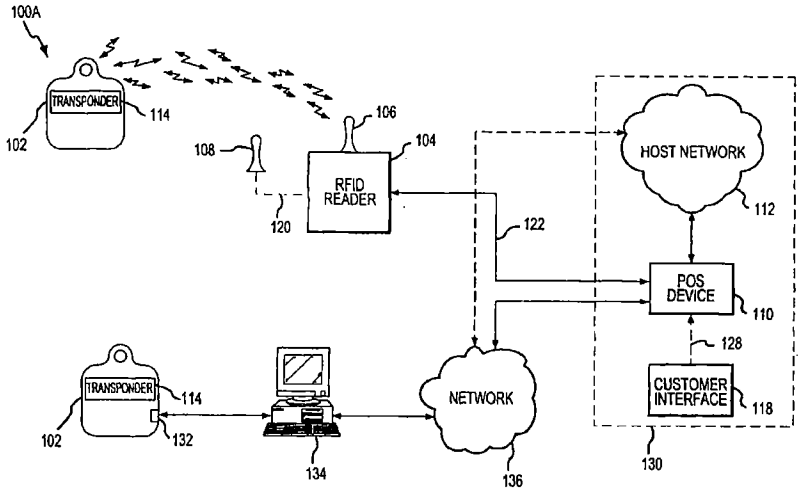
(72) Inventors: BERARDI, Michael, J.; 7770 NW 50th Street, #306, Lauderhill, FL 33313 (US). BLIMAN, Michal; 4 Dogwood Circle, Matawan, NJ 07747 (US). BONALLE, David, S.; 77 Rose Hill Avenue, New Rochelle, NY 10804 (US). ELWOOD, Jennifer, Anne; 115 East 34th Street, Apt. #8-G, New York City, NY 10016 (US). HOOD, Matthew, C.; 1112 LaFayette Road, Wayne, PA 19087 (US). ISENBERG, Susan, E.; 201 West 74 th, 12 th, New York City, NY 10012 (US). MAYERS, Alexandra; 49 Grove Street, #5-B, New York City, NY 10014 (US). SAUNDERS, Peter, D.; 3710 East Palisade Drive, Salt Lake City, UT 84109 (US). SCHEDING, Kathryn, D.; 12301 Clover Avenue, Los Angeles, CA 90066 (US). SHAH, Sejal, Ajit; 230 East 30th Street, #11-J, New York City, NY 10016 (US). WILLIAMSON, John, R.; 302 Pavonia Avenue, Jersey City, NJ 07302 (US).

(74) Agent: SOBELMAN, Howard, I.; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS



(57) Abstract: A transporter-reader payment system includes a fob (102) including a transponder (114), and a RFID reader (104) for interrogating the transponder (102). The system may further include a personalization system (134) for populating onto the fob (102) and RFID reader (104) identifying information and security and authentification keys which may be used during mutual authentication of the fob (102) and the reader (104) and for completing a transaction. In exemplary operation, the fob (102) and RFID reader (104) may be personalized, the fob (102) may be presented to the RFID reader (104) for interrogation, the fob (102) and reader (104) may engage in mutual authentication, and fob (102) identifying information may be provided to the reader (104) for transaction completion. In another exemplary embodiment, operation of the transponder-reader payment system may be controlled by an activation circuit. Further, the fob (102) may be responsive to multiple interrogation signals.

WO 03/007623 A3

SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
10 April 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US02/21903

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04Q 1/00; G05B 19/00
US CL : 705/17, 18; 340/5.52,5.6, 5.82

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 705/17, 18; 340/5.52,5.6, 5.82

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 6,073,840 A (MARION) 13 June 2000, Abstract and description of figures 4a,4b,5 and 6	1,6,7,36-38,50,52-62 --- 2-5,8-35,39-49
X --- Y	US 5,519,381 A (MARSH) 21 May 1996, column 3 lines 55 to column 4 lines 55	50 --- 2-5,8-35,39-49

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
04 October 2002 (04.10.2002)	30 DEC 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Brian A Zimmerman Telephone No. 703-305-4700

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 January 2003 (23.01.2003)

PCT

(10) International Publication Number
WO 03/007623 A3

(51) International Patent Classification[7]: H04Q 1/00, G05B 19/00

(21) International Application Number: PCT/US02/21903

(22) International Filing Date: 10 July 2002 (10.07.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/304,216 10 July 2001 (10.07.2001) US

(71) Applicant: AMERICAN EXPRESS TRAVEL RELATED SERVICES COMPAGNY, INC [US/US]; American Express Tower, World Financial Center, New York, NY 10285-4900 (US).

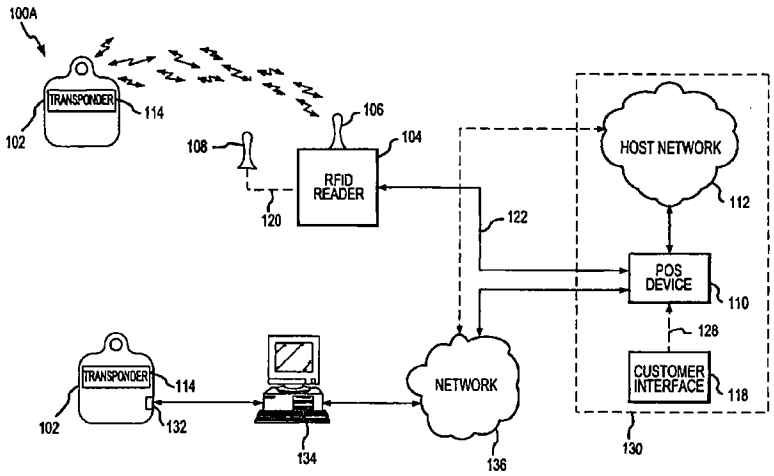
(72) Inventors: BERARDI, Michael, J.; 7770 NW 50th Street, #306, Lauderhill, FL 33313 (US). BLIMAN, Michal; 4 Dogwood Circle, Matawan, NJ 07747 (US). BONALLE, David, S.; 77 Rose Hill Avenue, New Rochelle, NY 10804 (US). ELWOOD, Jennifer, Anne; 115 East 34th Street, Apt. #8-G, New York City, NY 10016 (US). HOOD, Matthew, C.; 1112 LaFayette Road, Wayne, PA 19087 (US). ISENBERG, Susan, E.; 201 West 74 th, 12 th, New York City, NY 10012 (US). MAYERS, Alexandra; 49 Grove Street, #5-B, New York City, NY 10014 (US). SAUNDERS, Peter, D.; 3710 East Palisade Drive, Salt Lake City, UT 84109 (US). SCHEDING, Kathryn, D.; 12301 Clover Avenue, Los Angeles, CA 90066 (US). SHAH, Sejal, Ajit; 230 East 30th Street, #11-J, New York City, NY 10016 (US). WILLIAMSON, John, R.; 302 Pavonia Avenue, Jersey City, NJ 07302 (US).

(74) Agent: SOBELMAN, Howard, I.; Snell & Wilmer L.L.P., One Arizona Center, 400 East Van Buren, Phoenix, AZ 85004-2202 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PAYMENT USING RADIO FREQUENCY IDENTIFICATION IN CONTACT AND CONTACTLESS TRANSACTIONS



(57) Abstract: A transporter-reader payment system includes a fob (102) including a transponder (114), and a RFID reader (104) for interrogating the transponder (102). The system may further include a personalization system (134) for populating onto the fob (102) and RFID reader (104) identifying information and security and authentification keys which may be used during mutual authentication of the fob (102) and the reader (104) and for completing a transaction. In exemplary operation, the fob (102) and RFID reader (104) may be personalized, the fob (102) may be presented to the RFID reader (104) for interrogation, the fob (102) and reader (104) may engage in mutual authentication, and fob (102) identifying information may be provided to the reader (104) for transaction completion. In another exemplary embodiment, operation of the transponder-reader payment system may be controlled by an activation circuit. Further, the fob (102) may be responsive to multiple interrogation signals.

WO 03/007623 A3

SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *with amended claims*

(88) Date of publication of the international search report: 10 April 2003

Date of publication of the amended claims: 31 July 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

[Received by the International Bureau on February 28, 2003 (28.02.03): original claims 1-62 replaced by amended claims 1-59 (pages 29-40)]

1. A transponder-reader payment system comprising:

a. a Radio Frequency Identification (RFID) reader operable to provide a radio frequency (RF) interrogation signal for powering a transponder system, receiving a transponder system RF signal, and communicating a transponder system account data related to said transponder system RF signal to a merchant system, said RFID reader including,

i. a first interrogator for providing a first RF interrogation signal;

ii. a RFID authentication circuit in communication with said interrogator;

iii. a RFID database, in communication with said RFID authentication circuit, said database operable to store at least one of a RFID reader identifying data, a transponder system decryption security key, a RFID reader and encryption security key and a transponder authentication key;

iv. at least one of a serial interface and a universal serial bus (USB) interface; and

v. a RFID protocol/sequence controller in communication with at least one of said first interrogator, said RFID authentication circuit, said RFID database, and said USB interface, said RFID protocol/sequence controller configured to facilitate control of the order of operation of said interrogator, said RFID authentication circuit, said RFID database, and said USB interface.

2. A system according to claim 1 further comprising:

a. a transponder system operable to receive said first RF interrogation signal, authenticate said first RF interrogation signal, and transmit said transponder system account data, said transponder system comprising:

i. a first transponder responsive to said RF interrogation signal;

ii. a first transponder system antenna configured to receive said first RF interrogation signal;

iii. a second transponder responsive to a second RF interrogation signal, said first RF interrogation signal different from said second RF interrogation signal;

iv. a second transponder system antenna configured to receive said second RF interrogation system;

v. a transponder system authentication circuit in communication with at least one of said first transponder and said second transponder; and

vi. a transponder system database in communication with said transponder system authentication circuit.

3. A system according to claim 2, wherein said transponder system further includes:

a. a transponder system USB interface; and

b. a transponder system protocol/sequence controller in communication with at least one of said first transponder, said second transponder, said transponder system USB interface, said transponder system authentication circuit, and said transponder system database, said transponder system protocol/sequence controller configured to control the order of operation of said first transponder, said second transponder, said transponder system authentication circuit, said transponder system database, and said transponder system USB interface.

4. A system according to claim 1, wherein said RFID reader further includes:

a. a second interrogator, said second interrogator operable to send a second RF interrogation signal; and

b. a RFID communications interface configured to communicate with a merchant system, said communications interface operable to provide said transponder system account data.

5. A system according to claim 4, wherein said RFID reader further includes a first antenna in communication with said first interrogator and a second antenna in communication with said second interrogator, wherein said first antenna is operable to provide said first RF interrogation signal to said first transponder and said second interrogator is operable to provide said second RF interrogation signal to said second transponder.

6. A system according to claim 1, wherein said RFID database is operable to store a transponder system personal identification number (PIN).

7. A system according to claim 5, wherein said RFID reader further comprises at least one of a RFID internal antenna, and a RFID external antenna, said RFID internal antenna and said RFID external antenna configured to provide at least one of said first RF interrogation signal and said second RF interrogation signal.

8. A system according to claim 3, wherein said transponder system protocol/sequence controller is responsive to at least one of said first RF interrogation signal and said second RF interrogation signal, said transponder protocol/sequence controller controlling the sequence of operation at least one of said transponder system authentication circuit, said transponder system database, and said transponder system USB interface in response to at least one of said first RF interrogation signal and said second RF interrogation signal.

9. A system according to claim 3, wherein said transponder system protocol/sequence controller is configured to activate said transponder system authentication circuit in response to said first RF interrogation signal, said transponder system authenticating circuit configured to provide an encrypted RF interrogation signal, said transponder system authentication circuit configured to provide said encrypted RF interrogation signal to said first transponder for providing to said RFID reader.

10. A system according to claim 9, wherein said RFID reader is configured to receive said encrypted RF interrogation signal, said transponder system protocol/sequence controller

activating said transponder system authentication circuit in response to said encrypted RF interrogation signal.

11. A system according to claim 10, wherein said RFID database is configured to provide a transponder system decryption key to said RFID authentication circuit in response to said encrypted RF interrogation signal, said transponder system decryption key for use in decrypting said encrypted RF interrogation signal, providing a decrypted RF interrogation signal, said transponder system decryption key provided to said RFID reader based on an unique transponder identification code.

12. A system according to claim 11, wherein said RFID authentication circuit is configured to compare said decrypted RF interrogation signal and said RF interrogation signal to determine whether a match exists.

13. A system according to claim 12, wherein said RFID protocol/sequence controller is configured to activate at least one of said USB interface and said RFID communication interface where said RFID authentication circuit matches said decrypted RF interrogation signal and said RF interrogation signal.

14. A system according to claim 13, wherein said transponder system protocol/sequence controller activates said transponder system authentication circuit in response to at least one of said first RF interrogation signal and said second RF interrogation signal.

15. A claim according to claim 14, wherein said transponder system authentication circuit is configured to provide a transponder authentication code to at least one of said first transponder and said second transponder for providing to said RFID reader.

16. A system according to claim 15, wherein said RFID reader is configured to receive said transponder authentication code, said RFID protocol/sequence controller activating said RFID authentication circuit in response to said transponder authentication code, said RFID authentication circuit configure to encrypt said transponder authentication code.

17. A system according to claim 16, wherein said RFID reader is configured to provide said encrypted authentication code to said transponder system.

18. A system according to claim 17, wherein said transponder system database is operable to store at least one of a transponder system identification data, a RFID reader decryption security key, and a transponder system account data.

19. A system according to claim 18, wherein said transponder system database is configured to provide said RFID reader decryption security key to said transponder system authentication circuit in response to said encrypted authentication code, said RFID reader decryption key for use in decrypting said encrypted transponder authentication code and providing a decrypted transponder authentication code.

20. A system according to claim 19, wherein said transponder system authentication circuit is configured to compare said decrypted transponder authentication code and said transponder authentication code to determine if a match exists.

21. A system according to claim 20, wherein said account data is in magnetic stripe format.

22. A system according to claim 21, wherein said transponder system transaction account data is pre-encrypted.

23. A system according to claim 22, wherein said transponder system database is configured to provide said pre-encrypted transponder system account data to said RFID reader where said transponder system authentication circuit matches said decrypted transponder authentication code and said transponder authentication code.

24. A system according to claim 23, wherein said RFID communications interface is configured to provide said transponder system PIN and said pre-encrypted transponder system account data where said transponder authentication code matches said decrypted

transponder authentication code, and said decrypted RF interrogation signal matches said RF interrogation signal.

25. A system according to claim 24, wherein said transponder system further comprises a switch, said switch operable to enable or disable operation of said transponder system.

26. A system according to claim 25, wherein said switch is configured to place the transponder system in at least one of a selectivity mode and an inclusivity mode.

27. A system according to claim 25, wherein said switch is mechanical.

28. A system according to claim 25, wherein said switch is configured to respond to a logic circuit.

29. A system according to claim 2, wherein said transponder system further includes an internal power source.

30. A system according to claim 29, wherein said switch is in communication with said internal power source, said switch responsive to said internal power source.

31. A system according to claim 29, wherein said transponder system further includes a biometric circuit, said biometric circuit in communication with said internal power source.

32. A system according to claim 25, wherein said switch is a biometric circuit, said biometric circuit operable to enable or disenable operation of said transponder system.

33. A system according to claim 32, wherein said biometric circuit is configured to place said transponder system in one of a selectivity mode and an inclusivity mode.

34. A system according to claim 7, wherein said RFID reader includes a RFID PIN keypad, said RFID PIN keypad configured to receive said transponder PIN, said RFID reader configured to compare said transponder PIN to said received transponder PIN, said RFID reader operable to provide at least one of said received transponder PIN, said transponder PIN, or a verification of said received transponder PIN, verification of received transponder

PIN provided where said RFID reader matches said transponder PIN to said received transponder PIN.

35. A system according to claim 7, wherein said RFID reader is configured to provide said transponder PIN to a payment authorization center for verification of said transponder PIN.

36. A system according to claim 34, wherein said merchant system includes a merchant system PIN keypad, said merchant system PIN keypad configured to receive said transponder PIN from said merchant system PIN keypad, said merchant system configured to provide said transponder PIN to said payment authorization center for verification.

37. A system according to claim 31, wherein said biometric circuit is configured to provide a biometric data verification response, said biometric circuit configured to provide said biometric data verification response to at least one of said RFID reader and said merchant system, wherein said biometric data verification response is an identification verification data.

38. A system according to claim 3, further comprising a personalization system operable to initialize at least one of said transponder system and said RFID reader to transponder-reader payment system parameters.

39. A system according to claim 38, wherein said personalization system is in communication with said transponder system using at least one of a USB connector and RF communications.

40. A system according to claim 39, wherein said personalization system is in electrical communications with said RFID reader.

41. A system according to claim 40, wherein said personalization system is operable to populate at least one of said RFID reader identifying data, transponder system decryption security key, RFID encryption security key, and transponder PIN on said RFID database.

42. A system according to claim 41, wherein said personalization system is operable to populate at least one of said transponder system identification data, a RFID reader decryption security key, a transponder encryption authentication security key, a transponder system transactional account data, and a transponder system authentication security key onto said transponder system database.

43. A system according to claim 2, wherein said RFID reader is operable to initialize said transponder.

44. A system according to claim 2, wherein said RFID reader is in RF communication with said transponder system, said RFID reader operable to populate at least one of said transponder system identification data, a RFID reader decryption security key, a transponder system transactional account data onto said transponder system database.

45. A transponder-reader payment system including a transponder system operable to receive a first RF interrogation signal, and authenticate said first RF interrogation signal, said transponder system comprising:

a. a first transponder responsive to said first RF interrogation signal;

b. a second transponder responsive to a second RF interrogation signal, said first RF interrogation signal different from said second RF interrogation signal;

c. a first transponder system antenna configured to receive said first RF interrogation signal; and

d. a second transponder system antenna configured to receive said second RF interrogation signal.

46. A system according to claim 45, wherein said transponder system further includes at least one of a transponder system USB interface, transponder system authentication circuit, and a transponder system serial interface.

47. A transponder-reader payment system comprising:

a. a RFID reader operable to provide a RF interrogation signal for powering a transponder system, receiving a transponder system RF signal, and communicating a transponder system account data related to said transponder system RF signal to a merchant system, said RFID reader including:

i. a first RFID reader antenna in communication with a first interrogator for providing a first RF interrogation signal; and

ii. a second RFID reader antenna in communication with a second interrogator, for providing a second RF interrogation signal;

b. a transponder system operable to receive at least one of said first and second RF interrogation signal, authenticate said received interrogation signal, and transmit a transponder system account data, said transponder system comprising:

i. a first transponder antenna in communication with a first transponder, said first transponder responsive to said first RF interrogation signal; and

ii. a second transponder antenna in communication with a second transponder, said second transponder responsive to said second RF interrogation signal.

48. A system according to claim 47, wherein said RFID reader includes at least one of a a RFID reader authentication circuit, a RFID reader serial interface and a RFID reader USB interface, and said transponder system includes at least one of a transponder system USB interface, transponder system authentication circuit, and a transponder system serial interface.

49. A method of transponder-reader payment comprising the steps of:

a. providing a transponder system, the transponder system responsive to a plurality of interrogation signals, the transponder system storing at least one of an account data, an account name, and account expiration date, the transponder system including at least a first transponder responsive to a first interrogation signal and a second transponder responsive to a second interrogation signal; and

b. providing a RFID reader, said reader configured to provide at least one of the interrogation signals.

50. A method according to claim 49, further comprising the steps of:

a. encrypting the transponder system account data;

b. initializing the transponder system;

c. initializing the RFID reader;

d. mutually authenticating the RFID reader and the transponder system;

e. providing the encrypted account data from the transponder system to the RFID reader;

f. decrypting the encrypted account data; and

g. providing the decrypted account data to a merchant system.

51. A method according to claim 50, wherein mutual authenticating includes the RFID reader authenticating the transponder system, and the transponder system authenticating the RFID reader.

52. A method according to claim 51, wherein mutual authentication includes:

a. providing an interrogation signal from the RFID reader to the transponder system;

b. encrypting the interrogation signal at the transponder system to form an encrypted authentication interrogation signal;

c. providing the encrypted authentication interrogation signal to the RFID reader;

d. decrypting the encrypted authentication interrogation signal at the RFID reader, decrypting including using a transponder system decryption security key;

e. matching the interrogation signal to the decrypted interrogation signal;

f. providing an authorization code from the transponder system to the RFID reader;

g. encrypting the authorization code at the RFID reader to form an encrypted authorization code;

h. providing the encrypted authorization code to the transponder system;

i. decrypting the encrypted authorization code at the transponder system, decrypting including using a RFID reader decryption security key; and

j. matching the authorization code to the decrypted authorization code.

53. A method according to 52, where initializing the transponder system includes populating at least one of a transponder system identification data, a RFID reader decryption security key, a transponder system transactional data, and an encrypted transponder PIN onto a transponder system database.

54. A method according to claim 53, wherein initializing the RFID reader includes populating at lease one of a transponder system identification data, a RFID reader decryption security key, a transponder system transactional data, and an encrypted transponder PIN onto a transponder system database.

55. A method according to claim 49, wherein initializing the RFID reader includes populating at least one of a RFID reader identifying data, a transponder system decryption security key, a RFID encryption security key, and a transponder PIN onto a RFID database using a USB interface.

56. A method according to claim 53, wherein initializing the transponder system includes populating at least one of a transponder system identifying data, a RFID reader decryption security key, and a transponder system transaction data using a USB interface.

57. A method according to claim 49, wherein initialing the transponder system, includes initializing said transponder system using a RFID reader.

58. A method according to claim 54, including using a switch to enable the transponder system, the switch consisting of at least one of a mechanical switch, a logic switch, and a biometric switch.

59. A method according to claim 58, including providing a secondary identification in response to a request from a merchant system.